

火绒安全软件 6.0

用户操作手册

2025/04/14



- 公 司:北京火绒网络科技有限公司
- 地 址:北京市朝阳区北苑路北京文化创意大厦 B 座 9 层
- 网 址: https://www.huorong.cn
- 电话: 400-998-3555



版权声明

本文件所有内容版权受中国著作权法等有关知识产权法保护,为北京火绒网络科技有限公司(以下简称"火绒安全")所有。

未经火绒安全允许,不得转载本文件内容,否则将视为侵权。转载或者引用本文内容请注明来源及原作者。

对于不遵守此声明或者其他违法使用本文件内容者,火绒安全依法保留追究其法律责任的权利。

另外,火绒安全保留修改本文件中描述产品的权利。如有修改,不另行通知。



目录

•	产品	概述	6
٠	基码	功能说明	7
		软件安装	7
		● 获取安装包	7
		● 运行安装包	7
		● 安装完成	9
		程序主界面1	1
		病毒查杀1	3
		● 启动扫描	3
		● 查杀速度1	4
		● 启用 GPU 加速1	5
		● 查杀完成后自动关机1	6
		● 发现威胁1	7
		● 处理威胁1	8
		● 隔离区2	0
		● 信任区2	3
		防护中心2	7
		● 病毒防护	7
		● 系统防护3	1
		● 网络防护3	9
	۶	访问控制4	2
		● 密码保护4	2



	● 上网时段控制	43
	● 网站内容控制	44
	● 程序执行控制	48
	● USB 设备控制	.51
	● IP 协议控制	.53
	● IP 黑名单	56
۶	安全工具	58
۶	软件应用商店	.59
۶	托盘程序	60
	● 托盘消息	61
۶	常规设置-基础设置	62
	● 快捷操作	62
	● 密码保护	64
	● 色彩模式	69
	● 游戏模式	70
	● 应用商店图标展示	71
	● 用户体验计划	72
۶	管理设置	73
۶	软件卸载	75
进降	阶功能说明	77
۶	病毒查杀	77
	● 信任风险文件	77



	● 查杀设置	79
\triangleright	防护中心	82
	● 病毒防护	82
	● 系统防护	95
	● 网络防护	121
\triangleright	安全日志	137
	● 功能介绍	137
	● 安全日志设置说明	139
\triangleright	软件升级	140
	● 升级方式	140
	● 软件升级设置说明	144
总约	结	146





火绒安全软件是针对互联网 PC 终端设计的安全软件,本软件与 Microsoft 合作,适用 于 Windows XP (sp3 及以上)、Windows VISTA、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows 11、Windows Server (2003 sp1 及以上)的消费者防病 毒软件。

火绒安全软件主要针对杀、防、管、控这几方面进行功能设计,主要有病毒查杀、防护 中心、访问控制、安全工具四部分功能。由拥有连续十五年以上网络安全经验的专业团队研 发打造而成,特别针对国内安全趋势,自主研发拥有全套自主知识产权的反病毒底层核心技 术。

火绒安全软件基于目前 PC 用户的真实应用环境和安全威胁而设计,除了拥有强大的自 主知识产权的反病毒引擎等核心底层技术之外,更考虑到目前互联网环境下,用户所面临的 各种威胁和困境,有效地帮助用户解决病毒、木马、流氓软件、恶意网站、黑客侵害等安全 问题,追求"强悍的性能、轻巧的体量",让用户能够"安全、方便、自主地使用自己的电 脑"。

6



◆ 基础功能说明

本部分将会为您介绍常用的软件功能,如病毒查杀、防护中心、访问控制以及各类安全设置等。让您对火绒安全软件基础功能的使用有所了解。满足您日常生活中的网络安全防护需求。

▶ 软件安装



您可以访问火绒官网获取最新安装包:https://www.huorong.cn/









您需要勾选阅读并接受许可协议&隐私政策,若您不同意,则无法使用本软件。

安装方式:

- 极速安装:火绒默认为极速安装,您可点击"极速安装"按钮直接进行安装,安装完成 后即可使用。
- 自定义安装:当您需要将火绒安装在指定磁盘位置时可以选择此方式,您可以点击"安装目录"。





注: 在展开的安装目录选择信息中, 点击右侧浏览可选择您要安装的位置。



■ 静待安装: 耐心等待安装完成。





■ 立即使用:安装完成后,点击"立即体验"即可启动火绒安全防护。



■ 重启服务:因隐私设备保护等服务项需要您重启设备后才能生效,您可以根据

自身需要随时选择重启。



▶ 程序主界面





	问题反馈	打开火绒安全官方论坛
	病毒上报	打开火绒安全官方论坛查看病毒样本上报途径说明
	关于我们	查看火绒安全软件的许可协议,隐私政策。
	检查更新	开始检查更新
快捷入	安全日志	打开安全日志页
	信任区	打开信任区
	隔离区	打开隔离区
		根据用户使用习惯和您当前计算机状态,在主页位置主动
主页	建议	向您推送火绒的使用建议或功能推荐;多条建议时支持切换;
		支持对单条建议直接打开和关闭该条建议(见下图)。



0		⊙ ⇒	:	×
•	已保护 21 天			
Ŧ	火绒正在保护您的电脑			
කී	快速直杀			
	 注 推荐操作 漏洞修复可以帮助您检查计算机是否存在漏洞,建议 定期扫描和修复 去扫描 我知道了 	/		
D				
ଡି	检查更新 安全日志 信任区 隔离区 版本:6.0.0.0 病毒库:	2023-03-3	18 09:5	6

≻病毒查杀

火绒病毒查杀能主动扫描在电脑中已存在的病毒、木马威胁。当您选择了需要查杀的目标,火绒将通过自主研发的反病毒引擎高效扫描目标文件,及时发现病毒、木马,并帮助您 有效处理清除相关威胁。

● 启动扫描

您可通过主页 (见下图) 按钮处,选择查杀方式,火绒支持【快速查杀】、【全盘查杀】、 【自定义查杀】3 种查杀方式,您选择合适的查杀方式后,可一键开启查杀。



0		⊙ ≂ – ×
•	已伊	税 21 天
Ŧ	火	绒正在保护您的电脑
ෂ		快速查杀 ^ 全盘查杀
		自定义查杀 西存在调调,建议
IJ		
ରେ	位直	思新 安全日志 信任区 隔离区 版本:6.0.0.0 病毒库:2023-03-18 09:56
~~~		
功能		说明
功能 快速查	۲. ج	<mark>说明</mark> 病毒文件通常会感染电脑系统敏感位置, 【快速查杀】针对这些敏感
功能 快速查:	杀	说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感 位置进行快速的查杀,用时较少,推荐您日常使用。
功能 快速查: 全盘查:	۲	说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感 位置进行快速的查杀,用时较少,推荐您日常使用。 针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发
功能 快速查: 全盘查:	آنان       آنان <th>说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感 位置进行快速的查杀,用时较少,推荐您日常使用。 针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发 现电脑中毒后进行全面排查。</th>	说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感 位置进行快速的查杀,用时较少,推荐您日常使用。 针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发 现电脑中毒后进行全面排查。
功能 快速查 全盘查 自定义	杀 杀 查杀	说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感位置进行快速的查杀,用时较少,推荐您日常使用。 针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发现电脑中毒后进行全面排查。 您可以指定磁盘中的任意位置进行病毒扫描,完全自主操作,有针对
功能 快速查: 全盘查: 自定义:	杀杀	说明 病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感 位置进行快速的查杀,用时较少,推荐您日常使用。 针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发 现电脑中毒后进行全面排查。 您可以指定磁盘中的任意位置进行病毒扫描,完全自主操作,有针对 性地进行扫描查杀。推荐您在遇到无法确定部分文件安全时使用。
功能         快速查:         全盘查:         自定义:	杀 杀 查	说明         病毒文件通常会感染电脑系统敏感位置,【快速查杀】针对这些敏感         位置进行快速的查杀,用时较少,推荐您日常使用。         针对计算机所有磁盘位置进行查杀,用时较长,推荐您定期使用或发         现电脑中毒后进行全面排查。         您可以指定磁盘中的任意位置进行病毒扫描,完全自主操作,有针对         性地进行扫描查杀。推荐您在遇到无法确定部分文件安全时使用。         在您选择查杀位置时,提供易感染区域选择项,针对计算机易感染位

### ● 查杀速度

火绒为您提供了【常规】速度查杀和【高速】查杀 (见下图) 两种模式供您选择。



0	快速查杀		④ ≃ - ×			
	正在进行快速扫描	正在进行快速扫描				
6	C:\Program Files (x86)\Windows Media Play	/er				
F	第規   高速   □   启用GPU加速 □	] 查杀完成后自动关机	已用时间:00:01:34			
$\odot$	1.00		P-1			
සී			டு			
-	引导区	系统进程	启动项			
			שורנאני			
		~				
	<u> </u>	<u>ک</u>	$(\circ)$			
	服务与驱动	系统组件	系统关键位置			
	等待扫描	等待扫描	等待扫描			
ଡି						
功能	说明					
常规	占用较少的系统资	占用较少的系统资源				
高速	占用较多的系统资	源,提高扫描速度 <b>。</b>				

### ● 启用 GPU 加速

勾选即启用,启用后反病毒引擎会在此次扫描的适当时机使用 GPU 进行计算,进而提升扫描效率 (仅 DirectX 11 及以上版本支持)。



0	快速查杀		0 ≈ - ×
	正在进行快速扫描	停止 暂停	
6	C:\Program Files (x86)\Windows Media Play	er	
Ē	「「「「「「「「「」」 信用GPU加速 □ □ 信用GPU加速 □	] 查杀完成后自动关机	已用时间:00:01:34
Ð		_	<b>P</b> -
සී			<u>ل</u>
	引导区	系统进程	启动项
	×±	11_1.1_1]12 (***	BUTCHE
		0	
	ξ ^Ω λ	<u>ک</u>	$\odot$
	服务与驱动	系统组件	系统关键位置
	等待扫描	等待扫描	等待扫描
ଡ଼			

## ● 查杀完成后自动关机

勾选即启用功能。勾选后火绒将在扫描完成时弹出关机提示(见下图),关机提示等待的时间为 25 秒,25 秒后将为您自动关闭电脑。在此期间您可点击"暂不关机"或"×"以取消自动关机。



0	快速查杀		0 ≈ - ×				
	正在进行快速扫描	停止 暂停					
6	C:\Program Files (x86)\Windows Media Player						
Ŧ	常規 高速 □ 启用GPU加速 □	直杀完成后自动关机	已用时间:00:01:34				
ෂ	引导区	系统进程	し				
			等待扫描				
	Ś	స	$\bigcirc$				
	服务与驱动	系统组件	系统关键位置				
	等待扫描	等待扫描	等待扫描				
Ø							
0	🤣 火绒安全 🛛 🕹 👋 👋						
病毒查杀已完成, 电脑即将于 25 秒后关机							
法但方表西立地 心舟子生							
·归1木1	请保存重要文档,以免丢失 立即关机 暂不关机						

### ● 发现威胁

当火绒在扫描中发现病毒时,会实时显示发现风险项的个数,您可通过【查看详情】(见 下图)实时查看当前已发现的风险项。点击【退出详情】即可返回病毒扫描页面。



### ● 处理威胁

火绒安全

当扫描到威胁后,火绒安全软件提供病毒处理方式的选择。

⇒ 【立即处理】: 对所选择的风险项,进行隔离处理(建议您操作此项)。



➡ 【全部忽略】:对扫描出的风险项目不做处理(见下图)。



将威胁文件处理完毕后,提示扫描完成(见下图),为您展示扫描概况,将上一步处理

的威胁添加至【隔离区】。

0	快速查杀 所有风险项目处理完成			<ul><li>③</li></ul>
9				
<b>[+</b> ]				
සී		$\checkmark$		
		$\sim$		
U	目 扫描对象: 216070 个		① 总用时:36:34:23	
	🛆 发现风险:45 项		🕑 处理风险:45 项	
ଡି				



● 隔离区

火绒会将扫描后清除的风险项文件,经过加密后备份至【隔离区】(见下图),以便您 有特殊需要时,可以主动从隔离区中重新找回被清除的风险项文件。

👂 安全项管理	里								×
信任团	<u> </u>	隔离区							
隔离区备份了经	经过安全处理的风险	佥项 , 占用磁	盘空间:100KB						
	搜索	Q							
🗌 风险项		类型	风险名称 🔅	隔离时间 🗘	分类	≎ 操作			
	Adobe Illustrat C:\Windows\Br	文件	HEUR:TrojanDown	2023/06/22 15:34	Web扫描		提取		
0 🚞	新建文件夹 C:\Windows\Br	文件	Trojan Downloader	2023/06/22 15:34	文件实时监控	恢复	提取		
0 🌐	网址 www.cctt.com	网址	HEUR:TrojanDown	2023/06/22 15:34	恶意行为监控	恢复	提取		
	Adobe Photos C:\Program Fil	文件	TrojanDownloader	2023/06/22 15:34	U盘保护	恢复	提取		
0 🖂	邮箱 huo163@.com	邮箱	TrojanDownloader	2023/06/22 15:34	下载保护	恢复	提取		
	进程uwryuqw C:\Windows\Br	进程	HEUR:TrojanDown	2023/06/22 15:34	邮件监控	恢复	提取		
n ≓	实例程序	<del></del>	TeninaPaunlaadae	2022/06/22 15:24	147~b+")##	atotas	-स्वास्त	misa	
功能	说明								
删除所选	将选	中的文化	牛从隔离区删除	余,文件不可物	灰复。				
恢复所选	将选	中的文	牛恢复到其原如	台位置,同时从	人隔离区册	删除该文	件。		
提取所选	将选	中的文化	件复制至指定目	目录。					



#### 隔离区可以在以下四个位置进入:

→ 1:在首页的下拉菜单中找到隔离区(见下图)。



→ 2: 点击主页快捷入口的隔离区按钮,进入隔离区(见下图)。



⇒ 3: 在处理风险项后的扫描报告页中可以找到隔离区(见下图)。



0	快速查杀			⊙
4	所有风险项目处理完成 ^{风脸已经备份华 隔离区}			完成
Ŧ		~		
සී		$\langle \checkmark \rangle$		
U	目 扫描对象: 216070 个		④ 总用时:36:34:23	
	△ 发现风险:45 项		🗹 处理风险:45项	
ହ				

→ 4: 在鼠标右键单击火绒托盘图标后显示的快捷菜单中也可以找到隔离区(见下图)。

🛛 🥠 火绒安全	
已保护您的计算机 2	2324天 进入
	× 隔离区 检査更新
■ 流量悬浮窗	
回 游戏模式	
安全设置 交	医流反馈 退出火绒

#### 隔离区设置

您可在【安全设置】-【常规设置】-【日志和隔离】中限制隔离区存储大小,勾选后, 超过存储限制或磁盘已满时自动移除最早的隔离项。



🥠 🕏	安全设置		₽		×
© \$	常规设置	安全日志设置			
1	基础设置	超过存储限制或磁盘已满时自动移除最早的日志			
1	查杀设置	日志保存天数不超过 7 天			
E C	日志和隔离	□ 存储大小限制 1024 MB			
4 1	软件升级	隔离区设置			
÷ 1	病毒防护	超过存储限制或磁盘已满时自动移除最早的隔离项			
88 ;	系统防护	☑ 存储大小限制 1024 MB			
⊕ <b>Þ</b>	网络防护				

● 信任区

您可将确认安全的文件/文件夹或网址添加到【信任区】(见下图)。受信任的项目将 不会被认为包含风险,也不会被病毒查杀以及病毒防护的各项功能检测。您也可以在信任区 中对已有的项目取消信任--选中数据【删除所选】。

🕖 安全	项管理						-		×
	隔离区	信任区							
病毒查杀	与病毒防护的扫描功能将。	跳过以下信任项							
	选搜索							添加	
	信任项		类型	\$ 备	注	: 操作			
	hrkill-1.0.0.87.exe C:\Users\15931\Des	ktop\应用程序\下载\传输	文件路径			编辑	删除		
	C:\Users\15931\Des	ktop\应用程序\下载\传输.	义计超位			<u>1993</u>	面体		



功能	说明
删除所选	不再信任选中的信任项
清除无效项	点击【搜索】右侧开关,选择【清除无效项】,可清除信任区中对
	应路径下已无该文件或文件夹的项目。
编辑	重新编辑所选信任项的信息
添加信任	将需要信任的文件夹/文件/网址添加至信任区

### 添加信任:

🦪 添加信任	×
信任类型	
文件	~
「信任内容	
	B
☑ 改变文件内容后信任依旧生效	
备注	
保存	取消



功能	说明			
信任类型	文件/文件夹/网址			
信任内容	选择要信任的文件/文件夹路径或填写网址地址			
改变文件内容	选择信任类型为文件类型时,可勾选此项,勾选后,您配置的信			
后信任依旧生	任文件将记录为文件指纹类型,改变文件内容后信任依旧生效。			
效				
备注	方便您辨别信任项,可不填写。			

#### 信任区可以在以下三个位置进入:

→ 1:在首页的下拉菜单中可以找到信任区(见下图)。

<b>&gt;</b>		⊙ ≂ - ×
		È 安全日志
<b>A</b>	已保护 21 于	
		☑ 信任区
	火绒正在保护您的电脑	♡ 检査更新
Ŧ		■ 语言设置 >
		[] 问题反馈
Ô	快速貸余 ◇	── 病毒上报
ത		① 关于我们
	< > 推荐操作	17
	漏洞修复可以帮助您检查计算机是否存在漏洞,建议 史#813卷60条6	/
	AE-MILLIBERH #8名 去扫描 我知道了	
		· 2023-03-18 09-56
୍ତ		. 2025 05 18 05.50



		0 ≅ - X
<b>^</b>	已保护 21 天	
Ŧ	火绒正在保护您的电脑	
කි	快速查杀	
	休 注 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 休 か か か か か か か ひ か ひ か ひ か ひ か ひ ひ か ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ ひ	12-
U	去扫描 我知道了	
୍ତି	检查更新 安全日志 信任区 隔离区 版本:6.0.0.0 病毒库	: 2023-03-18 09:56

→ 2: 点击主页快捷入口的信任区按钮,进入信任区(见下图)。

⇒ 3: 在鼠标右键单击火绒托盘图标后显示的快捷菜单中可以找到信任区(见下图)。

🕗 火绒i	受全	
已保护您的计	算机 2324 天	进入
	τ	× 隔离区
上 安全日 日全安	志 档	
☑ 流量悬清	7窗	$\overline{}$
网 游戏模式	t	$\overline{\bullet}$
安全设置	交流反馈	退出火绒



# ≻防护中心

火绒防护中心一共有三大安全模块,共包含 22 类安全防护内容。当发现威胁动作触发 设定的防护项目时,火绒将为您精准拦截威胁,避免计算机受到侵害。

<b>(</b> )	防护中心		0 ≅ - ×
	查看、管理各项安全防护功能	2 2	
ଜ	<b>育毒防护</b> 7项防护已开启	<b>病毒防护</b> 发现并清除病毒,保护计算机不受病毒侵害	
Ŧ		⑦ 文件实时监控	۵ 🦲
සි	系统的护 6项防护已开启	◎ 恶意行为监控	
	网络防护 7项 防护已开启	一回 内存防护	@
		₽ U盘保护	۵ 🦲
U		. 下载保护	@
		── 邮件监控	۵ 🦲
			@
ଡ			

### ● 病毒防护

病毒防护是针对电脑病毒设计的病毒实时防护系统。共包含文件实时监控、恶意行为监控、内存防护、U盘保护、下载保护、邮件监控、Web 扫描 7 项安全防护内容。



	防护中心		⊙ ≈ - ×
	查看、管理各项安全防护功能	1	
ជ	<b>济毒防护</b> 7项防护已开启	<b>病毒防护</b> 发现并清除病毒,保护计算机不受病毒侵害	
Ŧ		文件实时监控	@
කී	新教的計 6项防护已开启	◎ 恶意行为监控	۵
	网络防护 7项 防护已开启	一 内存防护	@
		₽ U盘保护	۵ 🦲
		- 下载保护	۵ 🦳
		▶ 邮件监控	۵ 🦲
		web扫描	<b>—</b> @
୭			

→ 1: 文件实时监控

文件实时监控将在文件执行,修改或者打开时检测文件是否安全,即时拦截病毒程序。 在不影响电脑正常使用的情况下,实时保护您的电脑不受病毒侵害。

当有威胁触发了【文件实时监控】时,火绒将自动清除病毒,并弹出提示弹窗(见下图)提示您。



⇒ 2:恶意行为监控

恶意行为监控通过监控程序运行过程中是否存在恶意操作来判断程序是否安全,极大提升电脑反病毒能力。

当有威胁触发了【恶意行为监控】时,火绒将弹出提示弹窗 (见下图)提示您。您可根



#### 据需要选择相应处理方式。

🥠 恶意行为监控		×
发现风险		
建议您立即处理		
发起程序: <mark>影</mark> <u>behav.js</u> 风险名称: Backdoor/Drateam.A 操作目标: 后门病毒 (Backdoor/Drateam.A)秘密开 黑客的控制端,将被感染主机变为可以被黑客控制的	放用于远程操控的道 "肉鸡"。	端口和权限,或主动连接
信任	暂不处理	立即处理 (43)

→ 3: 内存防护

内存防护功能是针对混淆类恶意代码攻击和无文件攻击的场景进行深度防护,及时发现

并阻止安全风险;当有威胁触发了【内存防护】时,火绒将自动清除病毒,并弹出提示弹窗 (见下图)提示您。



→ 4:U盘保护

U 盘保护功能会在 U 盘接入电脑时对其根目录进行快速扫描,及时发现并阻止安全风险,避免病毒通过 U 盘进入您的电脑。同时移动存储设备也会自动纳入文件实时监控等其他监控功能保护范围,全方位保护您电脑的安全。

当有威胁触发了【U盘保护】时,火绒将自动清除病毒,并弹出提示弹窗 (见下图)提



示您。



#### → 5: 下载保护

在您使用浏览器、下载软件、即时通讯软件进行文件下载时对文件进行病毒扫描,保护您的电脑安全。当有威胁触发了【下载保护】时,火绒将自动清除病毒,并弹出提示弹窗(见下图)提示您。



#### → 6:邮件监控

邮件监控会对所有接收的邮件进行扫描,当发现风险时,将会自动打包风险邮件至隔离 区,并发送一封火绒已处理的回复邮件。对于发送的邮件,若发现邮件中包含病毒,火绒直 接将终止您的邮件发送,并自动清除病毒邮件至隔离区,防止病毒传播。

邮件监控目前仅支持邮件客户端收发的邮件,但不会对邮件客户端做出任何修改。

当有威胁触发了【邮件监控】时,火绒将自动处理威胁,并在处理完成后弹出提示弹窗(见下图)提示您。



接收病毒邮件:



#### 发送病毒邮件:



参 7: Web 扫描

当有应用程序与网站服务器进行通讯时,Web 扫描功能会对使用 SSL 加密的数据进行 病毒扫描检测,并及时阻止其中的恶意代码运行。

当有威胁触发了【Web 扫描】时,火绒将自动处理威胁,并在处理完成后弹出提示弹 窗 (见下图) 提示您。



● 系统防护

系统防护模块用于防护电脑系统不被恶意程序侵害。系统防护共包含系统加固、应用加



固、风险软件监控、软件安装拦截、隐私设备保护、浏览器保护、联网控制、自定义防护 8 项安全防护内容。

0	防护中心		0	₽	-	×
	查看、管理各项安全防护功能					
රු	病毒防护 7项防护已开启	<b>系统防护</b> 针对计算机系统潜在弱点进行防护,同时控制应用程序行为,防止被恶意软件利	用			
÷		〔 系统加固	1	-	0	
R		□□ 应用加固		-		
	○ 网络防护 □ 万顷 防护已开启	风险软件监控	9	-		
₿		家件安装拦截	(	-		
		② 隐私设备保护	0	-		
		② 浏览器保护	(	-		
		10 联网控制		•		
$\odot$						

→ 1:系统加固

系统加固功能根据火绒提供的安全加固策略,当程序对特定系统资源操作时提醒用户可能存在的安全风险。

当有威胁动作触犯【系统加固】时,火绒会弹窗(见下图)提示您,您可以根据需要选择对这个动作的处理方式。





→ 2:应用加固

应用加固功能通过对容易被恶意代码攻击的软件进行行为限制,防止这些软件被恶意代码利用。当有程序触发相应规则时,应用加固会弹窗(见下图)提示您,由您来决定是否允许该程序进行此项操作。





⇒ 3: 软件安装拦截

火绒会根据用户举报,将出现未经允许安装到用户计算机行为的软件,加入到安装拦截 列表中,在其他用户安装相同软件时进行弹窗提示(如下图)。

软件安装拦截能有效的减少您在不知情的情况下被安装不需要的软件。





→ 4:风险软件监控

此功能可设置监控不同类型的风险软件,默认仅监控潜在不受欢迎软件;当潜在不受欢迎软件运行时,将会弹窗询问用户如何处理,弹出以下弹窗(如下图)。



🥠 风险软件监控 🛛 👔 🗙
发现潜在不受欢迎的软件
此软件存在骚扰或风险行为
发起程序: <u>示例程序.exe</u>
软件名称:示例程序
数字签名:示例程序网络科技有限公司
<b>推荐操作</b> :建议您仅阻止风险行为,选择后将在该 软件运行过程中实时监控并阻止风险行为
☑ 记住本次操作,下次自动处理
阻止执行
允许执行
限制风险行为(25)

⇒ 5: 隐私设备保护

火绒隐私设备保护默认选择"仅通知",当有电脑软件要启用您的摄像头或麦克风时弹窗 (见下图)提示您,您可以根据需要在隐私设备保护的保护设置中设置是否允许电脑软件 启用摄像头或麦克风。






➡ 6:浏览器保护

浏览器保护(见下图)能保护您的浏览器首页不被随意篡改,此外在您访问电商网站与 银行官网等网站时,自动进入网购保护模式,阻止支付页面被篡改等网购风险,为您的浏览 器提供更全面的保护。

当您进入购物网站的时候,火绒会弹出保护提示。如您不需要,可取消勾选网购保护中的【当访问购物网站时弹窗提示】选项。



→ 7: 联网控制

当您需要阻止某程序联网,或者希望自行管控电脑中所有程序是否联网时,您可以通过 联网控制功能很好地管控电脑程序的联网行为。

该功能默认不启用,开启后任意程序进行联网时,联网控制都会弹出弹窗提示(见下图), 因此建议您根据需要决定是否开启此功能。

在弹出的联网控制弹窗中,您可以根据需要选择对这个动作的处理方式。





#### → 8: 自定义防护

自定义防护通过设置自定义防护规则能精准控制各项软件的执行,精准保护您不希望修改的文件、注册表等。有能力的用户可以通过自行编写防护规则,个性化的增强电脑防护能力。

当有威胁动作触犯【自定义防护】中的规则时,火绒会弹窗提示,您可以根据需要选择 对这个动作的处理方式。





● 网络防护

网络防护主要保护计算机在使用过程中,对网络危险行为的防御。网络防护共包含网络入侵拦截、横向渗透防护、对外攻击拦截、僵尸网络防护、暴破攻击防护、Web 服务保护、恶意网址拦截 7 项安全防护内容。



	防护中心		⊙ ≏ – ×
	查看、管理各项安全防护功能	3	
රා	京毒防护 7项防护已开启	<b>网络防护</b> 在网络层面拦截属洞攻击、黑客入侵等各项安全威胁	
æ		网络入侵拦截	•
සී	新統助护 6项防护已开启	对外攻击拦截	۵ 🦲
	网络防护	<u>□</u> 僵尸网络防护	۵ 🦳
		- Web服务保护	۵ 🦲
J		(→ 横向渗透防护	<b>—</b> @
		22 暴破攻击防护	۵ 🦲
		□□ 恶意网址拦截	e 🦲
Ø			

→ 1:网络入侵拦截

当黑客通过远程系统漏洞攻击电脑时,网络入侵拦截能强力阻止攻击行为,保护受攻击的终端,有效降低系统面临的风险。

当发现有网络入侵行为时,火绒将自动阻止,并通过托盘消息通知您。

→ 2:横向渗透防护

主要防护内网 (局域网)中的其他已经中毒电脑对本机的渗透,阻断病毒木马的传播和 扩散。

当发现有横向渗透行为时,火绒将阻止渗透行为,并通过托盘信息通知您。

→ 3: 对外攻击拦截

对外攻击拦截功能与网络入侵拦截技术原理一致(都是通过识别漏洞攻击数据包),但 是侧重于拦截本机对其它计算机的攻击行为。

当发现您的电脑有对外攻击行为时,火绒将自动阻止,并通过托盘消息通知您。

→ 4: 僵尸网络防护



僵尸网络防护将检测网络传输的数据包中是否包含远程控制代码,通过中断这些数据包 传输以避免您的电脑被黑客远程控制。

当发现有僵尸网络行为时,火绒将自动阻止,并通过托盘消息通知您。

→ 5:暴破攻击防护

不法分子常常通过暴力破解登录密码等其他密码破解攻击获取密码进行远程登录。一旦 远程登录进入主机,用户可以操作主机允许的任何事情。

当有发现计算机受到密码破解攻击时,火绒将阻止攻击行为,并通过托盘消息通知您。

参 6: Web 服务保护

保护 Web 服务相关的软件,阻止针对这些软件的漏洞攻击行为。

当有发现计算机受到入侵时,火绒将记录攻击行为,并通过托盘消息通知您。

→ 7:恶意网址拦截

恶意网站拦截功能,可以在您访问网站时自动分辨即将访问的网站是否存在恶意风险, 如果存在风险将拦截访问行为,并告知您,避免您的电脑受到侵害。

当您在浏览网页的时候,访问到有恶意风险的网站,火绒将拦截网站并弹出提示(见下 图)。





# ≻访问控制

当有访客使用您的电脑时,您可以使用上网时段控制、程序执行控制、网站内容控制、 USB 设备控制、IP 协议控制、IP 黑名单这些功能对访客的行为进行限制。

0	访问控制	<b>0</b>
	通过设定规则,控制用户对电脑资源的访问	密码保护①
☆ ⊕	上网时段控制 已开启 控制计算机上网的时间段或者累计的上网时长	网站内容控制 已开启 限制计算机访问特定类型网站
*	<b>程序执行控制</b> 未开启 限制指定应用程序的执行	↓ ↓ USB设备控制 未开启 ↓ ♀ ↓ 限制未信任的USB设备接入计算机
	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	IP黑名单 ① 未开启 この 限制对指定IP的出站、入站请求
ල		

### ● 密码保护

在开启访问控制的各项功能后虽然已经可以限制电脑的使用,但是功能开关仍可被随意 修改。此时您可通过设置密码来解决。

在访问控制页面中点击【密码保护】,进入安全设置页面,设置密码保护。



● 上网时段控制



火绒上网时段控制可根据您设定的上网时间来对电脑联网功能进行控制。



当前提供两种限制方式: 【控制上网时段】和【控制累计时间】。

功能	说明
控制上网时段	以一星期(一周)为周期,将可上网时间段作为限制,管控每天
	可上网的时间。
控制累计时间	将工作日(周一至周五)和周末(周六日)的累计上网时长作为
	限制,管控每天总上网时间。当发生流量变化时,就记为正在上网时
	间。
功能开关	开启,即上网时段控制功能生效。
	关闭,即上网时段控制功能未生效。

超出限定上网时间时,将弹出弹窗提示(见下图),并断网。您可点击【设置】或打开 火绒安全软件解除上网时段控制。

💋 上网时段控制	×
当前时段不允许使用网络	
时段控制:07:00-09:00	
	设置

● 网站内容控制

火绒网站内容控制可以限制计算机访问指定网址,达到屏蔽该网站的目的。限制访客访 问不受您信任的网站。



0		访问控	制 > 网站内容控制	•	≠ - ×
		限制计算	章机访问特定类型网站 <b>一〇</b>		
ណ៍		j	功能设置 自定义规则 999+		
Ŧ		网站类型			
		▣ 新	闻网站		
			购网站		
		回不	良网站		
5		☺ 游	戏网站		
Ô					
功能			说明		
功能开	¥		开启,即网站内容控制功能生效。		
			关闭,即网站内容控制功能未生效。		
网站类型开关		Ŧ关	功能开关开启后:		
			开启,即所选网站类型网站内容控制功能生效。		
			关闭,即所选网站类型网站内容控制功能未生效。		
自定义	规贝	IJ	您可自定义添加需要屏蔽的网址,点击后打开添加挂	截网	址弹窗。

除了火绒内置了 6 项常用的基础规则, 您还可根据需要通过【自定义规则】添加其他 需要屏蔽的网址。



0	访	问控制 > 网站(	内容控制				٢	₽	·	×
	限制	间计算机访问特定。	类型网站 🌕							
ជ្		功能设置	自定义规则 999+							
Ŧ									添加	
		〕 控制网站				状态	\$ 括	岼		
<u>8</u>	C	〕   自定义网址1				$\bigcirc$	貓	輯		
	C	] 自定义网址2				$\bigcirc$	编	備		
	C	] 自定义网址3				$\bigcirc$	编	絹		
		] 自定义网址4				$\bigcirc$	貓	闢		
	C	] 自定义网址5					编	闢		
		] 自定义网址6					编	闢		
	C	] 自定义网址7					编	镧		
		] 自定义网址8					維	闢		
~		] 自定义网址9					编	禰		
(ତ୍ର		〕 白⇔♡扇+ŀ1∩						曲		
功能		说明								
		~~ //								
添加		添加需要	要屏蔽的网址,	点击后打开	F添加拦截I	网址弹窗	(见下	图	)。	
编辑		编辑选中	中规则							
删除所	选	删除所有	与选中的规则							
功能开	¥	您添加的	的自定义规则,	必须在网站	5内容控制 <del>;</del>	开启时才会	主效,			
		您可通过	过每条规则后的	状态开关,	自定义调整	整规则是	否生效	Z.		



Ø 网站内容控制	×
自定义网址1	
多个网址通过换行进行区分,支持通配符"*' '>' (必填)	
保存取消	

功能	。 说明
规则名	您可以自定义当前规则名称
规则内容	填写要拦截的网址。
	多网址通过换行区分,每一行为一个网址。
	网址支持通配符* ?, 比如 www.*.com : 表示开头为 www.开始, 以.com
	结尾的所有网站都禁止访问。
保存	保存此规则
取消	关闭弹窗

当电脑访问受限网站时,火绒将拦截网址,并在浏览器中显示拦截提示(见下图)。在 网页提示中超出范围的信息将用...代替,鼠标移入时将显示全部信息。



## ● 程序执行控制

火绒安全

在访客使用您电脑的过程中,若您希望限制访客使用您的部分软件;此时可开启程序执 行控制,以限制某个或某类程序在电脑中的使用。

0	访问控制 > 程序执行控制		<b>⊙</b>
	限制指定应用程序的执行 🦲		
ស្	功能设置 自定义规则 999+		
Ē	应用程序	开启项	状态
(+)	<ul> <li>● 单机游戏</li> </ul>		── 共4项 ^
	4567软件		
	4567软件		
	4567软件		
ŏŏ	4567软件		
បា	🔇 网络游戏		● 共2项 ∨
	♀ 休闲益智游戏	未开启	● 共12项 ~
	☆ 対战平台     ☆	未开启	● 共 32 项 ∨
	● 影音娱乐		
	₩天工具		● 共12项 ∨
Ô	<b>一</b> 代理工具		



功能	说明
功能开关	开启,即程序执行控制功能生效。
	关闭,即程序执行控制功能未生效。
状态开关	橙色表示开启:程序执行控制将阻止该规则下的程序启
	动。
	灰色表示关闭:该规则内程序不受程序执行控制限制。
	您也可以选择某一类中的单个程序设置是否开启执行
	控制功能。
自定义规则	如您需要添加自定义屏蔽的程序,点击进入自定义规则
	页面(见下图)。

0	访问控制 > 程序执行控制	⊙ ≈ - ×	
	限制指定应用程序的执行 🦲		
ណ៍	功能设置 自定义规则 999+		
Ŧ	删除所选		添加
	口程序	\$ 状态	\$操作
	口		
	口 wxxx程序 C\Windows\apppatch\AppPatch64		
[]	Adobe Photoshop CC 2019 C:\Program Files (x86)\Common Files\System		
	Adobe Illustrator CC 2023 C:\Windows\BrowserCore\en-US		
	Adobe Premiere Pro 2024 C:\Program Files (x86)\Common Files\System		
Ø	C:\Users\Public\Downloads		



功能	说明
功能开关	您添加的自定义规则,在程序执行控制功能开启时生
	效。
删除	删除选中程序
状态开关	开启:程序执行控制将阻止该规则下的程序启动。
	关闭:该规则内程序不受程序执行控制限制。

#### 点击【添加】,选择您需要阻止运行的程序,点击保存即可。



当执行受限制程序时,火绒将弹窗提示您,并阻止程序执行。点击【详情】会打开火绒的程序执行控制页面,若您已设置密码,还会在页面上弹出输入密码提示弹窗。





### ● USB 设备控制

火绒 "USB 设备控制"提供了控制 USB 外接设备的接入与使用的功能。用户可以分别 对不同 USB 设备类型加限制。

0	访	访问控制 > USB设备控制   ① マ - ×				×				
	限制	制未信	任的USB设备排	_{送入计算机} (						
ណ៍		访问记	录 999+	设备白名单	999+					
E.	іš	设备名称			设备类型	接入时间		操作		
Ð	设	备名称x:	xxx		U盘存储设备	2023/06/30 15:34				
s@2	ម្ល	备名称x:	xxx		U盘存储设备	2023/06/26 15:34				
	设	备名称x:	xxx		便携设备 🛈	2023/06/25 15:34				
	设	备名称x:	xxx		USB无线网卡	2023/06/22 15:34				
ōŏ	设	备名称x:	xxx		打印机	2023/06/22 15:34				
<u></u>	ម្ល	诸名称x:	xxx		便携设备 🛈	2023/06/22 15:34				
	设	备名称x	xxx		USB有线网卡	2023/06/22 15:34				
	ម្ល	备名称x	xxx		打印机	2023/06/22 15:34				
	设备名称xxxx			便携设备 🛈	2023/06/22 15:34					
	ម្ល	备名称x	xxx		光駆	2023/06/22 15:34				
Ó	ig	诸名称x:	ххх		打印机	2023/06/22 15:34				
功能			说明							
<b>功能开关</b> 开启		开启	,即 USE	3 设备控制功	能生效。					
			关闭	,即 USE	3 设备控制功	能未生效。				
设备类型		便携	设备、U	SB 无线网卡、	USB 有线网卡、打	印机、	光驱。	,		
<b>操作</b> 允许		: 您允许i	该类 USB 设备	备接入计算机,允许原	言, 设备	备进入	白名	单,		



下次接入不再通知您。

用户可将信任的 USB 设备添加到白名单中,白名单中的设备接入计算机时,将不会拦

截。				
	访问控制 > USB设备控制			<b>⊙</b> ≈ - ×
	限制未信任的USB设备接入计算机 🦲			
ស	访问记录 999+ 设备白名单 999+			
F	取消信任			
, v	□ 信任的设备 ≎	设备类型	连接状态	操作
8	□ 设备名称xxxx	U盘存储设备	未连接	
	□ 设备名称xxxx	U盘存储设备	未连接	取消信任
Bô	□ 设备名称xxxx	便携设备 ①	未连接	
	□ ··········□ ························	USB无线网卡	未连接	取消信任
	□ 设备名称xxxx	打印机	未连接	
	□ 设备名称xxxx	USB有线网卡	未连接	取消信任
	□ 设备名称xxxx	便携设备 ①	未连接	
	□ 设备名称xxxx	打印机	未连接	取消信任
â	□ 设备名称xxxx	光驱	未连接	
U CO		@推设会 ∩	丰许控	1773年1月1日
功能	说明			
重命名	鼠标移入设备名称显示编辑图标,点击可对设备进行重命名。			
取消信任	不再信任勾选的设备,并从信任列表中移除。			

当接入的 USB 设备不在白名单列表内时,火绒将弹出阻止窗口(见下图)。点击【详 情】会打开火绒的 USB 设备控制页面,若您已设置密码,还会在页面上弹出输入密码提示 弹窗。





### ● IP 协议控制

IP 协议控制是在 IP 协议层控制数据包进站、出站行为,并且针对这些行为做规则化的 控制。您可以自己编写 IP 协议规则,并且管理 IP 协议控制的相关规则。当发现有触发 IP 协议控制规则的操作时,火绒根据用户设置的规则放过或阻止,并通过托盘消息通知用户。

0	访问控制	딄 → IP协议	控制			Q	, ≏	- ×
	在IP协议原	层进行网络访问	可控制 ① 🦲					
ជ្		搜索	۹				ŗ	赤加
_	口规	则名称	应用程序 🗘	说明	优先级 💲	状态 📫	操作	
[+]		办议规则1	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	10		编辑	
		办议规则2	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	20		编辑	
88	MAI 🗌	办议规则3	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	20	lacksquare	编辑	
(C)	MAI 🗌	办议规则4	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	10		编辑	
	MAI 🗌	办议规则5	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	20		编辑	
	MAI 🗌	办议规则6	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地IP:任意IP 本地端口:任IP	20	lacksquare	编辑	
ଡ		办议规则7	D/hrome//211	操作:放行 方向:所有 协议:TCP/ 本地印:任意IP 本地端口:任IP	20		编辑	
功能	ថ	兑明						
搜索		支持通	通过规则名称	、应用程序和说明	搜索规则	,并实时	展示	搜索结
	牙	見。						



状态开关	开关亮色表示规则启用,开关灰色表示规则未启用。		
编辑	编辑勾选规则		
删除	删除所有勾选的规则		
导入	点击搜索右侧图标,选择导入后,选择需要导入的规则,点击确定		
	等待规则导入完成。		
导出	将导出所有勾选的规则,点击后选择保存位置点击确定,等待导出		
	完成。		
添加	点击【添加】进入 IP 协议控制规则添加页面(见下图)。		
功能开关	开启,即 IP 协议控制功能生效。		
	关闭,即 IP 协议控制功能未生效。		



🍠 IP协议规则		×
规则模版:	默认配置	~
规则名称:	IP协议规则	
应用程序:		
操作:	放行	~
方向:	所有	~
协议:	TCP 传输控制协议	~
本地IP:	默认:任意IP	0
本地端口:	默认:任意端口	0
远程IP:	默认:任意IP	0
远程端口:	默认:任意端口	0
优先级:		
	保存	取消

功能	说明
规则模板	为您提供了多个常用规则模板,选择后可快速设置添加规则页面。
规则名称	您可以自定义此规则名称
应用程序	选择适用的应用程序,不填写默认为针对所有应用程序。
操作	针对触发符合下列设置的条件行为,是放行、放行(不记录日志)
	还是阻止。
方向	控制联网方向
协议	选择适用的网络协议



本地 IP	设置电脑本地的物理 IP。可填写 IPv4(表示范围使用"_")和		
	Ipv6(可缩写),支持 CDIR,多个 IP 请用";"分隔。		
本地端口	设置电脑本地的物理端口。多个端口请用";"分隔。		
远程 IP	设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"_")		
	和 lpv6(可缩写),支持 CDIR,多个 IP 请用";"分隔。		
远程端口	设置需要访问的远程端口。多个端口请用";"分隔。		
优先级	选择该条规则优先级, 当 IP 协议的规则冲突时优先执行优先级较		
	高的规则。优先级1为最高级。		
保存	保存此规则		
取消	关闭 IP 协议控制规则添加页面,返回至 IP 协议控制规则列表首		
	页,不保存规则。		

按照上图中填写的规则进行保存,产生的规则含义是:

放行所有进出站采用 TCP 协议,并且通过本地全部 IP 和端口访问所有远程 IP 和端口 的行为,规则优先级为 1。

### ● IP 黑名单

当您的电脑有不受欢迎的 IP 访问时,您可以将这些 IP 添加到 IP 黑名单中,当发现有 IP 黑名单中地址的请求数据包时,火绒将直接丢弃,并通过托盘消息通知您。



0	访问控制 > IP黑名单
	限制对指定IP的出站、入站请求 ① 📒
ស	副除所选 搜索
	□ 远程IP
Ŧ	□ 192.168.1.2-192.168.1.255 本地IP 编辑 删除
	□ 192.168.1.2-192.168.1.255 本地P 编辑 删除
	□ 192.168.1.2-192.168.1.255 本地IP 编辑 删除
	□ 192.168.1.2-192.168.1.255 本地IP 编辑 删除
őð	□ 192.168.1.2-192.168.1.255 本地IP 编辑 删除
	□ 192.168.1.2-192.168.1.255 本地P 编辑 删除
୍ତି	L 192.168.1.2-192.168.1.255 本地IP 编辑 删除
-1.615	
功能	
搜索	支持通过远程 IP 和备注搜索规则,并实时展示搜索结果。
编辑	编辑选中规则
删除	删除所有选中的规则
导入	点击搜索右侧图标,选择导入后,选择需要导入的规则,点击确定等
	待规则导入完成。
导出	将导出所有勾选的规则,点击后选择保存位置点击确定,等待导出完
	成。
添加	点击【添加】弹出 IP 黑名单添加弹窗(见下图)



IP黑名单	×			
多个IP换行输入","或 ";" IP范围输入 "- "				
备注文字,可不填写				
保存取消				

功能	说明		
远程 IP	填写您需要屏蔽的 IP 地址可填写 IPv4 (表示范围使用"-")和 IPv6		
	(可缩写),支持 CIDR,多个 IP 请换行输入 。		
备注	方便您辨识规则,可不填写。		
保存	保存当前规则,添加至 IP 黑名单规则列表中。		
取消	点击关闭弹窗,不保存规则。		

# ≻ 安全工具

火绒还为用户提供了 14 个实用工具:漏洞修复、系统修复、弹窗拦截、垃圾清理、启 动项管理、文件粉碎、右键管理、断网修复、流量监控、修改 HOSTS 文件、ARP 防护、 DHCP 检测、安全分析工具、专杀工具,协助用户管理广告弹窗、启动项、右键菜单、流 量、清理垃圾和修复系统故障。针对局域网环境的 ARP 攻击和 DHCP 劫持问题,还提供了 ARP 防护和 DHCP 检测小工具,有效解决局域网环境下的常见问题。



<b></b>	安全工具		<b>0</b>
	常用工具		
ିନ୍ଦ			
<b>[+</b> ]	拖拽到此		
කී	系统工具		
	<b>漏洞修复</b> 扫描并修复系统漏洞	系统修复 修复因病毒等导致的系统异常	·····································
	中 垃圾清理 清理各种系统垃圾	○ 启动项管理 合动项管理 管理各类软件的开机自启动	文件粉碎 强制删除或彻底粉碎文件
	→ 右键管理   管理文件、桌面右键菜单		
0	网络工具		

# ▶ 软件应用商店

提供了火绒应用商店的快捷入口,非内置软件,您可自行选择是否下载火绒应用商店。



支持在安全设置-基础设置中配置是否显示该快捷入口,以及是否接收应用商店的通知。



▶ 托盘程序

火绒启动后会在电脑后台实时保护您的电脑,此过程中火绒程序进程将在托盘系统中继续运行,节省电脑资源。您可通过系统托盘区域,在需要火绒的时候方便快捷的找到火绒。 左键单击系统托盘图标,将显示火绒安全软件主界面。



右键单击系统托盘图标,将显示右键快捷菜单。

全安秘火 🄇	
已保护您的计算机 2324	4天 进入
信任区	▼ 隔离区
安全日志	☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆
□ 流量悬浮窗	
四 游戏模式	
安全设置 交流	反馈 退出火绒

功能	说明
进入	进入火绒安全软件主界面
信任区	快速进入信任区
隔离区	快速进入隔离区



安全日志	点击打开安全日志,安全日志详细介绍请在进阶功能
	说明-安全日志中查看。
检查更新	启动升级程序,检查软件版本情况。
流量悬浮窗	可快速开启或关闭流量悬浮窗,默认不开启。
游戏模式	默认不开启,开启后火绒将按推荐操作自动处理提示
	信息,不再弹出提示弹窗。
软件设置	快速打开软件设置页面
交流反馈	访问火绒官方论坛,您可在论坛中反馈您遇到的问题。
退出火绒	关闭火绒安全,停止火绒对电脑的保护。您也可以自
	行选择退出的时间,若时间结束且您持续处于开机状态,
	火绒将会重新自启(见下图)。



## ● 托盘消息

火绒将各类非重要的消息为您统一收至托盘消息中。当您收到新的消息时,您只需鼠标 移入系统托盘中火绒图标,即可显示火绒的托盘消息。



点击底部的【清除所有通知】可清空当前托盘消息。



# ▶ 常规设置-基础设置

● 快捷操作





功能	说明
把"病毒扫描"加入右键菜单	文件右键菜单中支持快速自定义扫描该文件
显示流量悬浮窗	勾选即在电脑右侧显示流量悬浮窗
显示 U 盘悬浮窗	计算机中插入 U 盘后, 显示 U 盘悬浮窗。
显示 U 盘托盘图标	计算机中插入 U 盘后,任务栏中显示 U 盘托盘
	图标。
开启托盘消息	开启后,鼠标悬浮火绒托盘图标显示托盘消息。
隐藏最近三天程序的运行记录	勾选后将在隐私设备保护保护、联网控制、程序
	执行控制,添加规则页面下次打开时隐藏最近三天运
	行的程序。隐藏后界面按照暂无最近运行的程序来显
	示。默认不勾选。



▶ 密码保护 (

您可通过设置密码防止有人未经您的允许修改部分防护功能的配置。

### ⇒ 1:设置密码

打开启用开关,弹出密码设置页面。

0	安全设置		₽	-	×
	常规设置	快捷操作			
	基础设置	☑ 把"病毒扫描"加入右键菜单			
	查杀设置	☑ 显示流量悬浮窗			
	日志和隔离	☑ 显示U盘悬浮窗			
	软件升级	□ 显示U盘托盘图标			
Ð	病毒防护	□ 显示托盘消息提示			
	系统防护	□ 隐藏最近三天程序的运行记录			
	网络防护	密码保护     密码设置     设置密保       修改关键设置时需要您输入密码进行授权       色彩模式     明亮模式			
		游戏模式			
		<ul> <li>并启后, 立即进入游戏模式</li> <li>7 开启后, 在以下时机进入游戏模式</li> </ul>			

在密码设置页 (见下图) 中, 输入您需要设置的密码, 勾选您希望密码保护的保护范围, 填写完毕后点击【保存】即可, 密码保护将立即生效。设置密码后会提示您是否设置密保 (见 下图)。



🕖 密码设置			×
*密码保护			
新密码:	请输入新密码	Ø	
确认密码:	请再次输入新密码	Ø	
*保护范围 访问控制	完全设置 □ 安全日志 □ 隔离区 □ 信任区 退出程序 □ 卸载程序		
	保存	取消	
<ul><li>浸 提示</li></ul>	密码设置成功,建议您立即设置 密保可在密码保护中进行设置。	× 密保	
	前往设置	取消	

当您在密码保护的范围中进行任意操作时,均会弹出输入密码的弹窗(见下图),要求

您输入设置的密码才能进行相应操作。



🧭 火绒安全		×
*当前操作需要您输入安全密码		
		ø
	确定	取消

### ⇒ 2:设置密保

当您忘记密码时,可通过回答密保问题重新设置密码;若您忘记密保问题答案,将无法通过密保问题找回密码,请您谨记密保问题及答案。

🥠 设置密保		×
为了避免遗忘,请您	填写真实信息,这将帮助您以后通过密保问题找回密码	
*问题—:	如:我出生的城市	
*答案:	北京 (不区分大小写)	
*问题二:	如:我最好的朋友	
*答案:	小明 (不区分大小写)	
*问题三:	如:我的第一只宠物叫什么	
*答案:	旺财 (不区分大小写)	
		下—步



🥖 密码设置		×
以下是您刚刚设置的	的密保问题,请做出回答并谨记。	
问题一:	我出生的城市	
*答案:		
问题二:	我最好的朋友	
*答案:		
问题三:	我的第一只宠物叫什么	
*答案:		
		2.AU
	± 2 7	61-26

点击"完成"按钮完成密保问题验证,验证通过后,密保设置成功。

#### ⇒ 3:修改密码

需要修改密码或修改密码保护范围时,您可在常规设置-基础设置中点击【密码设置】 (见下图)再次打开密码设置页。进行修改密码或修改保护范围。





#### → 4:关闭密码保护

您需要在常规设置-基础设置中关闭密码保护功能开关,并且通过密码验证后,即可关

闭密码保护。





0	安全设置				₽		×
	常规设置	快捷操作					
	基础设置	✔ 把"病毒扫描"加入右键菜单					
	查杀设置	✓ 显示流量悬浮窗					
	日志和隔离	✓ 显示U盘悬浮窗					
	软件升级	□ 显示U盘托盘图标					
Đ	病毒防护	🗆 🦪 火绒安全	×	7			
	系统防护	□ 当前操作需要您输入安全密码					
œ	网络防护	*******					
		· · · · · · · · · · · · · · · · · · ·	取消				_
		色h/metu		L.			
		◎ 暗黑模式 ○ 明亮模式					
		NenE4H-P					
		进入游戏模式后,检查停Windows更新互补推去火线弹圈用意					
		0 开启后,在以下的机进入游戏模式					

## ● 色彩模式

### 支持切换明亮模式和黑暗模式。

0	安全设置		₽	-	×
	常规设置	快捷操作			
	基础设置	☑ 把"病毒扫描"加入右键菜单			
	查杀设置	☑ 显示流量悬浮窗			
	日志和隔离	☑ 显示U盘悬浮窗			
	软件升级	□ 显示U盘托盘图标			
Ð	病毒防护	□ 显示托盘消息提示			
88	系统防护	□ 隐藏最近三天程序的运行记录			
¢	网络防护	<b>密码保护</b> 图 密码设置 设置密保 修改关键设置时需要您输入密码进行授权			
		<ul> <li>● 暗黑模式 ○ 明亮模式</li> </ul>			
		游戏模式 进入游戏模式后,将暂停Windows更新且不推送火绒弹窗消息 ● 开启后,立即进入游戏模式 ● 开启后,在以下时机进入游戏模式			



● 游戏模式

进入游戏模式后,默认暂停 Windows 更新,您可设置开启游戏模式开关后,具体什么时机开始不推送火绒弹窗消息,减少计算机卡顿。

🍠 安全设置	≂ – ⊡ ×
③ 常规设置 基础设置	□ 显示托盘消息提示 □ 隐藏最近三天程序的运行记录
查示设置 日志和陽离 软件升级	密码保护  密码设置 设置密保 修改关键设置时需要您输入密码进行授权
田 病毒防护     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     ○     □     ○     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □	<ul> <li>● 暗黒模式 ○ 明亮模式</li> </ul>
⊕ 网络防护	<ul> <li>游戏模式 ●</li> <li>进入游戏模式后,将暂停Windows更新且不推送火绒弹窗消息</li> <li>开启后,立即进入游戏模式</li> <li>开启后,在以下时机进入游戏模式</li> <li>程序全屏运行时进入</li> <li>指定程序项方时进入</li> </ul>
	应用商店图标展示 ● ✓ 接收应用商店通知(通知包含:火绒应用商店版本升级通知、软件升级通知)

功能	说明
开启后, 立即不推送火绒弹窗消息,	选中后, 开启游戏模式开关后, 将立即不推送弹
并减少计算机卡顿	窗消息,并减少计算机卡顿。
开启后,在以下时机不推送火绒弹	启游戏模式开关后,只有在所设置的特定情况下
窗消息,并减少计算机卡顿	才会不推送弹窗消息,并减少计算机卡顿。
程序全屏运行时	任意程序全屏运行时,自动开始不推送弹窗消
	息,减少计算机卡顿。
指定程序运行	指定的程序运行时,自动开始不推送弹窗消息,



	减少计算机卡顿,您可自己添加程序(见下图)。
进入游戏模式后,暂停 Windows	开启游戏模式开关后,暂停 Windows 更新。
更新	

秋京列表     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水     水					
		所选		· · · · · · · · · · · · · · · · · · ·	
		程序		操作	
		0	hrkill-1.0.0.87.exe C:\Users\15931\D	♪ Desktop\应用程序\下载\传输文件	
功俞	ie I			说明	
添加	IA			将指定程序添加到列表中	
删降	余			删除勾选的所有程序	

## ● 应用商店图标展示

您可通过设置此开关设置【首页】-【左侧导航栏】是否展示火绒应用商店的图标,以 及是否接收应用商店相关通知。

①:此开关默认打开,如您不需要展示,可设置为关闭状态。



②:接收应用商店通知:此项默认不勾选,如您需要接收火绒应用商店相关的通知,可 勾选,勾选后,【首页】-【左侧导航栏】火绒应用商店的图标处则接收商店相关通知,以 小红点角标形式提醒您。

0	安全设置		₽		×
	常规设 <u>置</u> 基础设置				
	<u>童杀没置</u>				
	软件升级	○ 明亮模式			
Ð	病毒防护	游戏模式 💽			
88	系统防护	进入游戏模式后,将暂停Windows更新且不推送火线弹窗消息			
$\oplus$	网络防护				
		应用商店图标展示 💽			
		□ 接收应用商店通知 (通知包含:火绒应用商店版本升级通知、软件升级通知)			
		用户体验计划			
		☑ 加入火绒用户体验计划 了解详情			

● 用户体验计划

您可设置是否加入火绒用户体验计划,参与用户体验改善计划后会自动上报火绒日常拦截威胁后产生的相关日志信息,这些信息只涉及威胁拦截日志相关内容,不涉及您的个人隐私信息或文件数据。


🚺 安全	设置		⇒ – ⊡ ×
<ol> <li>常规</li> <li>基础</li> </ol>	设置	☑ 并启托盖消息 □ 隐藏最近三天程序的运行记录	
<u></u> 査杀 日志	设置	密码保护	
软件:	升级		
土 病毒	師护	游戏模式 ● 进入答应地点 新认 暂停Windows 新新	
器 系统	跡护		
④ 网络	跡护		
		应用商店图标展示 💽	
		☑ 接收应用商店通知 (通知包含:火绒应用商店版本升级通知、软件升级通知)	
		用户体验计划	
		☑ 加入火线用户体验计划 了解详情	
		激活	舌 Windows



当您需要恢复设置的默认状态或是将规则设置导出并在另一台电脑上运行时,管理设置 就能很好的满足您的需求。您可在安全设置的右上角找到【菜单按钮】(见下图)。



0	安全设置		≂ – □ X		
0	常规设置	快捷操作			
	基础设置	☑ 把"病毒扫描"加入右键菜单			
	查杀设置	☑ 显示流量悬浮窗			
	日志和隔离	✓ 显示U盘悬浮窗			
	软件升级	□ 显示U盘托盘图标			
Ð	病毒防护	□ 显示托盘消息提示			
88	系统防护	□ 隐藏最近三天程序的运行记录			
⊕	网络防护	密码保护 ● 修改关键设置时需要您输入密码进行授权			
		<ul> <li>● 暗黑模式</li> <li>○ 明亮模式</li> </ul>			
		游戏模式			
		○ 开启后,在以下时机进入游戏模式			

功能	说明		
恢复默认设置	将回复您在火绒中修改的所有设置为默认状态,点击后弹出恢复		
	默认设置提示弹窗(见下图)。点击确定恢复默认设置,点击取消和		
	"×"关闭弹窗不恢复默认设置。		
导出设置	导出当前设置,点击后选择保存位置点击确定,等待导出完成即		
	可。		
导入设置	点击后选择需要导入的规则,点击确定等待规则导入完成,即可		
	导入设置。		





> 软件卸载

#### 火绒的卸载方法:

⇒ 方法一:

Windows7 通过"控制面板"—"卸载程序"中找到火绒,进行卸载。

Windows10 右键开始菜单选择"应用和功能",找到火绒,进行卸载。

Windows11 任务栏开始按钮弹窗中,选择所有应用,在火绒安全实验室下拉 菜 单中可以卸载火绒。

⇒ 方法二:可以在火绒安装目录下找到卸载程序,将火绒安全卸载。



	确定要卸载火绒吗?			
	<b>狠心卸载</b> 继续保护			
功能	说明			
狠心卸载	开始卸载,检测到隔离区存在文件时,弹出询问弹窗(见下图)。			
继续保护	关闭卸载程序,继续运行火绒。			
(	火绒安全 × 見否要提取隔离区内文件? 继续卸载将会清空隔离区			
	打开隔离区继续卸载			
功能				
打开隔离区	打开隔离区窗口,根据您的需要可提取或恢复隔离区文件。			
继续卸载	继续运行卸载程序			



🥠 火绒安全		- ×
	卸载完成,后会有期! ^{计算机已经失去安全防护}	
	立即重启 暂不重启	
	访问我们的网站: www.huorong.cn	

注:为确保卸载之后无残留文件,请在卸载之后重启电脑。

# ◆ 进阶功能说明

火绒为有一定知识背景的用户提供了可以手动自由控制杀毒软件以及电脑的方式,您可以通过调整火绒安全软件的设置,达到您自己想要实现的防护效果,更加精准地保护您的电脑。

## ≻病毒查杀

## ● 信任风险文件

在风险项中若含有您信任的文件, 您不想文件被清除同时又不想被反复扫描出来, 您可 在点击该文件的【详情】, 在弹出的【风险详情】中点击【信任文件】将该文件添加至信任 区。





🤣 风险详情	×
病毒类型:后门病毒 (Backdoor/Allaple.a)	
病毒描述: 秘密开放用于远程操控的端口和权限,或主动连接黑客的控 将被感染主机变为可以被黑客控制的"肉鸡"。	制端,
风险路径: C:\Users\15931\Desktop\应用程序\病毒样本\history.rar	
处理建议: 立即处理	
打开文件路径    信任文	件

您仍可再次点击已信任文件的【详情】,再点击风险详情中的【取消信任】已继续查杀

该风险文件。



<b>(</b> )	自定义查杀	<
	发现45项风险项目 過出洋情 停止 管停 警停	
$\Theta$	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Floxif蠕虫病毒\Floxif蠕虫病毒源文件.zip >> WormOrg.Floxif.A.dll	
_	□ 风险项目 状态	
( <del>+</del> )	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Allapl\Backdoor.Win32.Allaple.A.exe 后门病毒 Backdoor/Allaple.a 已信任 详情	
තී	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Alliance宏病毒\Virus.Word.Alliance.A.d,	
	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Al\WormOrg.Win32.Almanahe.A.exe	
G	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Ap们\Backdoor.Win32.Apdoor.A.dll 后门病毒 HEUR:Backdoor/ApDoor 已信任 详情	
	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Ap们\Backdoor.Win32.Apdoor.A.exe 术马病毒 HVM:Trojan/MalBehav.gen!A 已信任 详情	
	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> Aspid\Backdoor.Win32.Aspid.A.exe 术马病毒 HVM:Trojan/MalBehav.gen!C	
©	C:\Users\15931\Desktop\应用程序\病毒样本\history.rar >> As\Email-Worm.Win32.Assarm.A.exe 木马病毒 HVM:Trojan/MalBehav.gen!C	
	🥠 风险详情 X	
	病毒类型:后门病毒 (Backdoor/Allaple.a)	
	病毒描述: 秘密开放用于远程操控的端口和权限,或主动连接黑客的控制端, 将被感染主机变为可以被黑客控制的"肉鸡"。	
	风险路径: C:\Users\15931\Desktop\应用程序\病毒样本\history.rar	
	处理建议: 立即处理	

## ● 查杀设置

打开【安全设置】,点开选择常规设置-查杀设置,您可在查杀设置(见下图)中调整 病毒查杀的相关配置,如全盘查杀配置、快速查杀配置、修改病毒处理方式等。

打开文件路径

取消信任



0	安全设置		₽	-	×
	常规设置	全盘查杀设置			
	基础设置	□ 深度查杀压缩包中的木马病毒,并跳过大于 20 MB的压缩包(20M-9999M)			
	查杀设置	口 仅扫描指定扩展名文件 例如:.exe; doc.txt; zip			
	日志和隔离	□ 扫描网络驱动器			
	软件升级	朴法太大和業			
Đ	病毒防护				
88	系统防护				
$\oplus$	网络防护	自定义查杀配置			
		☑ 启用高级启发式扫描 ①			
		+ <b>-</b> 1世:八字			
		□ 启用GPU加速()			
		默认使用 iGame GeForce RTX 4090 Vulcan OC V 显卡进行GPU加速			
		病毒处理方式			
		〇 询问我			
		<ul> <li>自动处理</li> </ul>			

功能		说明
		勾选后,当压缩包大于您填写的数值时,扫描时
	压缩包扫描	将自动跳过,以加快扫描速度。
		若未勾选则在全盘查杀时扫描所有压缩包。
		勾选此项后,填写文件扩展名,填写格式示。
全盘查杀设置	仅扫描指定扩	例:.tmp;.txt;.log;.db 进行全盘查杀时, 仅扫描设置的
	展名文件	文件类型。
		多个文件类型之间用英文";"来隔开。
	扫描网络驱动	勾选后,在运行全盘查杀时,火绒会同时扫描映
	扫描网络驱动 器	勾选后,在运行全盘查杀时,火绒会同时扫描映 射好的网络磁盘中的文件。
	扫描网络驱动 器	勾选后,在运行全盘查杀时,火绒会同时扫描映 射好的网络磁盘中的文件。 勾选后,将在特定时机下自动进行快速扫描。



		的时机,可设置病毒处理方式,可设置计算机使用蓄
		电池时不扫描)。
自定义查杀配	启用高级启发	勾选后,自定义查杀时将会启用高启发式扫描,
置	式扫描	可高效查杀新型未知病毒。
		勾选后,反病毒引擎会在此次扫描的适当时机使
		用 GPU 进行计算,进而提升扫描效率 (仅 DirectX 11
	启用 GPU 加	及以上版本支持)。
扫描设置	速	针对存在多显卡的计算机,您可以设置使用哪个
		显卡去进行 GPU 加速;只有一个显卡的计算机,火绒
		默认使用唯一的显卡进行 GPU 加速。
	询问我	扫描出威胁后,显示发现的威胁文件,让您自主
		处理威胁。
病毒处理方式	自动处理	扫描出威胁后,火绒将根据推荐操作自动处理威
		胁文件。
	清除病毒时备	勾选后,清除的病毒会被备份到隔离区,方便您
	份至隔离区	进行查找,在出现误报误删的情况时,您可随时恢复
		误报误删的文件。
备份引导区		点击后选择保存位置,备份当前引导区。



>防护中心

### ● 病毒防护

有一定知识背景的用户可以通过对病毒防御模块的设置,来达到自己想要的防护效果。

#### ⇒ 1: 文件实时监控设置说明

通过设置可以调整【文件实时监控】所产生作用的形式,根据个人需要调整扫描时机、 排除文件、处理病毒方式、清除病毒备份隔离区、查杀引擎等内容,防止已经隐藏在电脑上 的病毒对电脑造成伤害。

- 衫 安全	设置	≂ – □ ×
<ul> <li>第歳時防护</li> <li>文件実时监控</li> <li>悪意行为监控</li> <li>内存防护</li> <li>以産保护</li> <li>下載保护</li> <li>邮件监控</li> <li>Web扫描</li> <li>第550防护</li> <li>① 网络防护</li> </ul>		文件实时监控 ————————————————————————————————————
		扫描时机         ○ 文件执行时扫描,不影响性能         ● 当文件被执行、修改时扫描,占用较多系统资源         ⑦ 文件发生所有操作时扫描,占用较多系统资源         病毒处理方式         ● 自动处理         ② 询问我         ● 自动处理         ② 清除病毒时备份至隔离区         排除         □ 不扫描描定程序的动作 例知:: C\Program File\t.exe;*.exe         高级         ② 启用通过 AMSI 对脚本和其它对象的高级扫描(启用此项可能导致部分游戏程序无法加载)
功能		说明
扫描时机		根据您的需要和电脑配置情况选择实时监控生效时机
病毒处 询问我		扫描出威胁后,弹出提示弹窗,让您来自主处理威胁。
理方式	自动处理	扫描出威胁后,火绒将根据推荐操作自动处理,不再询



		问您。
	清除病毒时备份	勾选后,清除的病毒会被备份到隔离区,方便您进行查
	至隔离区	找,防止误报误删。
排除		病毒实时监控的过程中,不扫描指定程序的文件操作。
		填写示例: C:\Program Files\Test\>.exe;*\Test.exe
		填写说明:需要填写要排除的程序路径,多条路径之间
		用英文";"分割。
		?:匹配1个任意字符。
		*:匹配0到多个任意字符。
		>:匹配除'\'和'/'以外的0到多个任意字符。
启用通过	± AMSI 对脚本和	勾选后,文件实时监控时,会启用 ASMI 进行高级扫描,
其他对象	象的高级扫描	结合火绒虚拟技术可以高效地查杀新型未知病毒,但会有误
		报;仅 Windows10 及以上系统支持。
		注意:AMSI 启动可能会造成部分游戏无法正常加载,
		建议避开游戏时机启用。
功能开关	ŧ	开启:文件实时监控功能生效。
		关闭:文件实时监控功能未生效。

#### → 2: 恶意行为监控设置说明

通过设置可以调整【恶意行为监控】发现威胁动作时是否自动处理,处理病毒与清除病 毒后备份隔离区等设置项目。



0	安全设置		⇒		×
© =	常规设置病毒防护	<b>恶意行为监控</b> ————————————————————————————————————			
	文件实时监控 恶意行为监控 内存防护 U盘保护	<ul> <li>病毒处理方式</li> <li>询问我</li> <li>自动处理</li> <li>清除病毒时备份至隔离区</li> </ul>			
88	下载保护 邮件监控 Web扫描 系统防护 网络防护	增强勒索病毒防护 <ul> <li>开启勒索病毒诱捕①</li> <li>休测到勒索行为时,还原被修改的文件</li> </ul>			

功能		说明			
病毒处理方	询问我	扫描出威胁后,询问您,让您来主动处理威胁。			
式	自动处理	扫描出威胁后,火绒将根据推荐操作自动处理,不再询			
		问您。			
	清除病毒时	勾选后,清除的病毒会被备份到隔离区,方便您进行查			
	备份至隔离	找,防止误报误删。			
	X				
增强勒索病毒	防护	勾选此项后,火绒会生成若干常见文件格式的随机文件,			
		病毒防护系统使用这些随机文件来诱捕勒索病毒,达到增强			
		防护的目的。			
检测到勒索行为时还原被		勾选此项后,当检测到勒索行为时,火绒会自动还原被			
修改的文件		勒索病毒修改的文件。但此功能首次安装火绒,勾选此功能			



	后需重启计算机才可生效。
功能开关	开启:恶意行为监控功能生效。
	关闭:恶意行为监控功能未生效。

#### ⇒ 3: 内存防护设置

通过设置可以调整【内存防护】功能的扫描灵敏度和病毒处理方式。

0	安全设置		₽	-	×
© [ <u>+</u>	常 常规设置 病毒防护	<b>内存防护</b> ————————————————————————————————————			
	文件实时监控 恶意行为监控 内存防护 U盘保护	<ul> <li>扫描灵敏度</li> <li>○ 低,系统性能优先</li> <li>◎ 适中,占用少量系统性能</li> <li>○ 高,扫描能力优先</li> </ul>			
88	下载保护 邮件监控 Web扫描 3 系统防护 9 网络防护	<ul> <li>病毒处理方式</li> <li>仅记录</li> <li>询问我</li> <li>自动处理</li> <li>注 清除病毒时备份至隔离区</li> </ul>			

功能		说明
扫描灵敏度		根据您的需要和电脑配置情况选择扫描灵敏度
	仅记录	扫描出威胁后,将不予以处理仅记录至安全日志中。
病毒处理	询问我	扫描出威胁后,弹出提示弹窗,让您来自主处理威胁。
方式	白油加加	扫描出威胁后,火绒将根据推荐操作自动处理,不再询
		问您。



	清除病毒时备	勾选后,清除的病毒会被备份到隔离区,方便您进行了	查
	份至隔离区	找,防止误报误删。	
功能开关		开启:内存防护功能生效。	
		关闭:内存防护功能未生效。	

#### → 4: U 盘保护设置说明

通过设置可以管理【U盘保护】的防护模式。调整可修复项目、病毒处理方式等内容, 防止病毒通过 U 盘感染您的电脑。

0	安全设置		₽		×
© =	常规设置病毒防护	U盘保护 ————————————————————————————————————			
	文件实时监控 恶意行为监控	<b>可修复项目</b> 一   一 </th <th></th> <th></th> <th></th>			
	內存防护 U盘保护 下载保护	压缩包扫描 □ 深度查杀压缩包中的木马病毒,并跳过大于 20 MB的压缩包(20M-9999M)			
	邮件监控 Web扫描	病毒处理方式			
00	系统防护	<ul> <li>回问我</li> <li>自动处理</li> </ul>			
	网络防护	<ul> <li>✓ 清涂病毒的省份至隔离区</li> </ul>			



功能		说明
可修复项目		勾选后将在自动扫描 U 盘的同时检测被病毒修改过的项
		目
压缩包扫描		勾选后,当压缩包大于您填写的数值时,扫描将自动跳
		过,以加快扫描速度。
病毒处理方	询问我	扫描出威胁后,弹出提示弹窗,让您来自主处理威胁。
式	自动处理	扫描出威胁后,火绒将根据推荐操作自动处理,不再询
		问您。
	清除病毒	勾选后,清除的病毒会被备份到隔离区,方便您进行查
	时备份至	找,防止误报误删。
	隔离区	
功能开关		开启: U 盘保护功能生效。
		关闭: U 盘保护功能未生效。

#### U 盘修复功能简介:

U 盘修复主要为您解决当清除部分 U 盘病毒后产生的两类遗留问题。一类是篡改 autorun 文件的病毒,在查杀后在可能会在 U 盘中遗留无效的 autorun.inf 文件;另一类是 部分病毒会隐藏您正常文件,释放伪装文件,诱导您传播病毒,当火绒查杀了这类病毒后会 清除病毒生成的伪装文件,但是会导致部分用户误以为杀毒软件把正常文件删除了。通过 U 盘修复可以删除无效的 autorun.inf 文件或检索 U 盘根目录中的隐藏文件与目录,引导您修 复。



#### U 盘修复功操作说明:

当 U 盘接入时发现可修复项目, 弹窗提示。



功能	说明
立即修复	修复选中的异常项目
暂不修复	关闭弹窗,不修复任何项目。

#### → 5: 下载保护设置说明

通过设置可以管理【下载保护】的生效方式,您可以根据自己的需要,对于下载的内容 进行有针对性的查杀,防止病毒通过互联网下载文件感染您的电脑。



🍠 安全设置		≂ – ⊡ ×
<ul> <li>常规设置</li> <li>病毒防护</li> </ul>	下载保护 🦲 💭 实时扫描通过浏览器、即时通讯软件下载的文件	
文件实时监控	<b>压缩包扫描</b> □ 深度查杀压缩包中的木马病毒,并跳过大于  20     MB的压缩包(20M-9999M)	
内存防护 U盘保护 下载保护 邮件监控 Web扫描	<ul> <li>病毒处理方式</li> <li>◎ 询问我</li> <li>○ 自动处理</li> <li>✓ 清除病毒时备份至隔离区</li> </ul>	
器系统防护 ⊕ 网络防护		

功能		说明
压缩包扫描		勾选后,当压缩包大于您填写的数值时,扫描将自动跳过,以加快扫描速度。
	询问我	扫描出威胁后,弹出提示弹窗,让您来自主处理威胁。
病毒处理	自动处理	扫描出威胁后,火绒将根据推荐操作自动处理,不再询问您。
方式	清除病毒时 备份至隔离 区	勾选后,清除的病毒会被备份到隔离区,方便您进行查 找,防止误报误删。
功能开关		开启:下载保护功能生效。 关闭:下载保护功能未生效。



#### ⇒ 6:邮件监控设置说明

通过设置可以管理【邮件监控】的生效方式,您可以根据自己的需要,对于发送、接受 邮件进行有针对性的查杀,防止病毒通过邮件附件感染您的电脑。

0	安全设置		⇒ –	ĸ
©	常规设置病毒防护	邮件监控 ————————————————————————————————————		
	文件实时监控 恶意行为监控 内存防护	保护范围 ✓ 接收邮件 ✓ 发送邮件		
	U盘保护 下载保护 邮件监控	邮件扫描 深度查杀压缩包中的木马病毒,并跳过大于 20 MB的压缩包(1M-20M)		
00	Web扫描	病毒处理方式		
	网络防护	<ul> <li>① 1000年</li> <li>② 自动处理</li> <li>② 清除病毒时备份至隔离区</li> <li>高级</li> </ul>		
		扫描指定协议及端口 配置规则		

功能		说明				
保护范围		您可根据需要自由勾选邮件监控保护范围				
邮件扫描		当邮件大于您填写的数值时,邮件扫描将自动跳过,不				
		予以扫描。				
	仅记录	发现病毒后火绒将不予以处理仅记录至安全日志中				
亡主机四子		发现病毒后,火绒将根据推荐操作自动处理,并记录至				
<b>病毒</b> 处埋万 式	目动处理	安全日志中。				
	备份至隔离	勾选后,清除的病毒会被备份到隔离区,方便您进行查				
	X	找,防止误报误删。				



	设置邮件监控扫描的协议及端口,点击【配置规则】进
言识	入协议端口的配置页面(见下图)。
同级	默认存在两个规则:25 端口 SMTP 协议以及 110 端口
	POP3 协议。
功能开关	开启:邮件监控功能生效。
	关闭:邮件监控功能未生效。

	) 曲科	牛监控	×	<
			·····································	
		端口	\$ 协议	
		110	POP3 编辑 删除	
		112	SMTP 编辑 删除	
		112	POP3 编辑 删除	
		110	POP3 编辑 删除	
e				
功能			说明	
编辑	ł		编辑勾选规则	
删除	ŧ		删除所有勾选规则	
添加	1		添加新的需要扫描的协议和端口,点击后会以弹窗形式让您新建一	条
			规则(见下图)供您填写添加。	
导入	•		点击搜索右侧图标,选择导入后,选择需要导入的规则,点击确定	等



	待规则导入完成。
导出	将导出所有勾选的规则, 点击后选择保存位置点击确定, 等待导出完
	成。

🕖 添加规则		- ×
*端口		
请输入端口		
协议		
SMTP		~
	保存	取消

功能	说明
保存	保存当前规则,添加至规则列表中。
取消	退出添加规则状态,不保存当前规则。

#### ➡ 7: Web 扫描设置说明

通过设置可以管理【Web 扫描】是否检测 https 协议端口和病毒处理方式,以及加密 扫描错误时处理方式,防止病毒通过您访问的网站感染您的电脑。





功能		说明		
病毒处理	仅记录	发现病毒后火绒将不予以处理仅记录至安全日志中		
方式	自动处理	发现病毒后,火绒将根据推荐操作自动处理,并记录至		
		安全日志中。		
	备份至隔离区	勾选后,清除的病毒会被备份到隔离区,方便您进行查		
		找。		
		开启后,支持检测 HTTPS 协议的端口。		
		1:火绒会默认跳过一些网站,您可通过【网站列表】		
		查看内置跳过的网站。		
加密链接扫描		2:火绒支持用户自定义扫描的 https 端口,默认扫描		
		443,如果您有其他 https 端口需要扫描,可点击【端口列		



	表】,管理扫描的端口列表。					
	3: 扫描范围:					
	①: 仅扫描可能存在风险的加密链接。					
	②:扫描全部加密链接(注意:此项开启可能导致部分)					
	程序无法正常联网)。					
	4:发生扫描错误时处理方式:					
	<ol> <li>①:火绒默认处理方式为弹窗询问,让您来自主处理。</li> </ol>					
	②: 您也可以选择扫描错误时将域名添加至排斥列表,					
	添加至排除列表后,后续加密扫描将自动跳过。					
	③:或者您可以选择扫描错误时忽略此域名,下次加密					
	扫描发生错误后,火绒将自动忽略,不再提示您。					
	5: 扫描排除域名: 如果您有信任的域名不需要进行加					
	密扫描,或需要将排除的域名从排除列表移除,您可在此处					
	管理排除域名裂变。					
	6:受信任的程序:如果您有信任的程序不需要进行加					
	密扫描,或需要将信任的程序从列表移除,您可在此处管理					
	信任的程序。添加到信任程序列表的程序,发生加密链接时,					
	默认不扫描。					
功能开关	开启:Web 扫描功能生效。					
	关闭:Web 扫描功能未生效。					



● 系统防护

有一定电脑知识背景的用户可以通过对系统防护模块的设置,配置相应规则,控制电脑中的程序对系统的修改与调整来达到对系统防护的效果。

#### → 1:系统加固设置说明

通过设置可以管理【系统加固】的生效规则,火绒针对计算机系统,进行规则内置,您 可以根据自己的需要,调整防护项目,防止电脑的各项系统设置被恶意程序篡改。

0	安全设置					≂ – ⊡	×
0	常规设置		13 -E-144 /= 07+175				
Ð	病毒防护	针对计算机杀死治住家	每辰1进行10分钟				
88	系统防护	基础防护					
				>_	-1		
	应用加固	文件防护	注册表防护	敏感动作防护	关键进程保护		
	风险软件监控	已开启7项	已开启7项	已开启7项	已开启 0 项		
	软件安装拦截	☑ 启动内置过滤规则(	D				
	隐私设备保护						
	浏览器保护	自动防护					
	联网控制	E					
	自定义防护	自动处理					
$\oplus$	网络防护	已开启7项					
		智能防护					
		☑ 启动系统免疫 ①					

功能		说明
基础防护	文件防护	保护基础文件不被篡改、破坏或恶意创建。
	注册表防护	防止特定注册表项目被恶意篡改
	关键进程保护	支持防护(关键的系统进程、IE 浏览器进程、资源管理
		器进程)对被保护的关键进程进行防篡改加固。
	启用内置过滤	监控针对系统的敏感行为,拦截高风险动作。保护系统



	规则	重要进程,不会被攻击利用。			
自动防护	自动处理	点击进入自动处理页面,调整自动处理规则。			
智能防护	启用系统免疫	勾选后,火绒将自动阻止针对系统关键进程、特殊方式			
		操作注册表、写物理内存等高危操作行为。			
功能开关		开启:系统加固功能生效。			
		关闭:系统加固功能未生效。			

#### ① 基础防护:

您可在基础防护中针对文件防护、注册表防护、执行防护、关键进程的防护的防护项目 进行修改调整。火绒为您默认配置了相应规则,您可根据需要自行调整,勾选您需要启动的 防护项目,选择对应的生效方式即可。防护项目对应说明可参看后方的防护说明内容。

如您需恢复默认配置状态,您可点击页面左下角的【恢复默认】按钮。

🤊 系统加固						×
文件防护	注册表防护	敏感动作防护 ①	关键进程	2保护		
					恢复	默认
防护项目	防护说明		处	理方式	状态	
Autorun配置文件	保护U盘不被	病毒文件侵染		😑 询问我		
恶意创建任务栏快捷方式	对一些软件的	同后台任务栏快捷方式创建进行拦截	<b>湖</b> 示	😑 自动阻止		
Hosts配置文件	保护Hosts配	置文件不被篡改		🕗 自动允许		
启动配置文件	保护启动配置	1文件不被破坏		😑 询问我		
关键系统文件	保护关键系统	保护关键系统文件文件不被篡改		😑 询问我		
IE快捷方式	保护IE快捷方	保护IE快捷方式不被篡改		😑 询问我		
桌面任务栏	保护桌面任务	保护桌面任务栏快捷方式不被篡改		😑 询问我		
桌面任务栏(利用系统组件)	对一些软件和	川用系统组件修改桌面任务栏进行拦	截	😑 询问我		
启动目录(扩展保护)	保护启动目录	保护启动目录不被恶意篡改		😑 询问我		
桌面任务栏(利用系统组件)	对一些软件和	川用系统组件修改桌面任务栏进行拦	截	😑 询问我		
域控共享目录	保护域控共享	目录不被随意创建文件		😑 询问我		



② 自动防护:

部分程序为了达到持续篡改系统某些配置的目的,会反复执行相同操作,为了不反复弹 窗提示拦截信息,打搅您的日常使用,所以提供了自动处理功能,您可以选择记住操作,减 少相同弹窗提示。同时我们开放了自主添加自动处理项目的功能,方便您自由管控。

	)自	动处理								×
									添加	
		程序				已选项目		操作		
		0	实例程序 C:\Wind	ows\apppatch\AppPatch64				编辑		
			xxxx程序 C:\Wind	ows\apppatch\AppPatch64				编辑		
		67								
		Ai	Adobe Il C:\Wind	lustrator CC 2023 ows\BrowserCore\en-US				编辑		
		Pr	Adobe P C:\Progr	remiere Pro 2024 am Files (x86)\Common Files\System				编辑		
		Xd	Adobe E C:\Users	xperience Design 2020 Public\Downloads				编辑		
		Ae	Adobe A C:\Wind	fter Effects 2020 wws\Containers\serviced				编辑		
功	能			说明						
编	辑			编辑选中规则						
删	除			删除所有选中规则						
清	除无	效规	则	删除所有无效的规则						
				无效规则判定:对应路径下已无该程序	茅。					
添	bO			添加需自动处理的规则,点击后切换3	宦汤	动规则可	ই (	见下	图)	您
				填写添加。						

🤣 自动处理							
发起程序: *					选择程序		
文件规则	注册表规则	敏感动作规则	关键进程规则				
请选择需要自动处理的	的防护项目,并设置生效方式						
✓ Autorun配置	文件			😑 自动阻止			
☑ 恶意创建任务	栏快捷方式			⊘ 自动允许			
✓ Hosts配置文化	(4			◎ 自动允许			
✓ 启动配置文件							
□ 关键系统文件				😑 自动阻止			
□ IE快捷方式				💿 自动阻止			
□ 桌面任务栏				😑 自动阻止			
□ 桌面任务栏(未	则用系统组件)			◎ 自动阻止			
□ 启动目录(扩展	<b>梨保护</b> )			😑 自动阻止			
一 保护对象:自动处理规	则必须开启对应的防护项目才能生效	X.					
				保存	取消		
功能	说明						
发起程序	选择控制操作	的程序					
保护对象	勾选需要自动	加阻止或自动允许	F的项目				
保存	保存当前规则	」,添加至规则歹	则表中。				
取消	切回自动处理	<b>即则列表,不例</b>	存当前规则。				

火绒安全 HUO RONG SECURITY





#### ★ 保存规则-规则冲突:

发现已存在相同发起程序的自动处理规则时您可以选择处理方式:

Į	🍠 自动处理			×			
	1) 发现已存在相同发起程序的自动处理规则,请选择您的处理方式!						
	合并:合并新规则 替换:旧规则的保	都将被保留 对象					
	旧规则的保护对象		新规则的保护对象				
	文件规则 防护项目:hosts配置文件 防护项目:恶意创建任务栏快捷方式 防护项目:启动配置文件 处理方式:自动阻止 注册表规则 防护项目:启动配置文件 处理方式:自动允许 敏感动作规则		文件规则 防护项目:hosts配置文件 处理方式:自动阻止 注册表规则 防护项目:启动配置文件 处理方式:自动允许 合并	替换			
1				省换			
功能		说明					
合并		合并新规则和旧规则的保护对象,新旧规则保护对象都保留。					
替换		旧规则的保护对象将全部被替,仅保留新规则的保护对象。					

#### ★ 自动添加-自动防护:

当危险行为触犯系统加固中生效方式为弹窗提示的规则时,会弹窗提示,如果您勾选【记 住本次操作】(下图),就会将自动添加规则到【自动处理】列表中,下次遇到相同问题, 则采取相同方式处理。



🕖 系统加固	×
发现程序试图操作 注册表防护项目	
发起程序:	结束进程
记住本次操作,下次自动处理	
阻止(45)	
允许	

#### → 2: 应用加固设置说明

加固类型中勾选,代表该防护规则开启,后面的图标为您电脑中对应安装的应用程序。

0	安全设置								₽		×
0	常规设置	应用	用加固 🛑								
Đ	病毒防护	控制	削应用程序的行为,防止被恶意:	软件利用	8						_
88	系统防护	加固	国类型								
	系统加固		Web服务器	0							
		Ø	数据库	<b>O</b>							
	风险软件监控		办公软件	×	1	•	•	-			
	软件安装拦截	Z	文档阅读器	7	<u>a4</u>	1					
	隐私设备保护		浏览器	0	0						
	浏览器保护		设计软件	9	×						
	联网控制		其他软件	9	0						
	自定义防护										
$\oplus$	网络防护										
8											

程序卸载后,对应图标消失。



#### → 3:风险软件监控设置说明

您可在风险软件监控设置中,设置限制【潜在不受欢迎软件】的哪些软件行为。设置【控

制风险工具】、【下载站下载器】、【远程控制工具】是否执行。



软件防护范围	下图)。
功能开关	开启:风险软件监控功能生效。
	关闭:风险软件监控功能未生效。



0	安全设置		≂ - □	×	
0	常规设置	风险软件监控 🦲			
Đ	病毒防护	扫描存在安全风险的程序软件,限制其风险行为权限			
88	系统防护	功能设置 自动处理规则 999+			
	系统加固	软件类型			
	应用加固 风险软件监控	潜在不受欢迎的软件①     限制此类软件的行为     限制此类软件的行为	防护范围 ^ 💽	1	
	软件安装拦截 隐私设备保护	防护项目	状态		
	浏览器保护	联网			
	联网控制	关键系统进程加载			
	自定义防护	最次販売位置文件			
⊕	网络防护				
		標以)) 见帝国从收 (合) 无法在我们仍要			
		AND			
0					
功能	it i	说明 			
状系	5	开启:自动阻止潜在不受欢迎软件的该行为。			
		关闭:允许潜在不受欢迎软件的该行为。			
恢复默认 状态全部恢复为开启状态					

检测到风险软件运行时,会弹出询问弹窗,如果您勾选【记住本次操作】(下图),就 会将自动添加规则到【自动处理】列表中,下次该风险软件再次运行时,则自动处理。



> 风险软件监控	>
发现潜在不受欢迎的软件	
此软件存在骚扰或风险行为	
发起程序:  示例程序.exe	
软件名称:示例程序	
数字签名:示例程序网络科技有限公司	
<b>推荐操作</b> :建议您仅阻止风险行为,选择 软件运行过程中实时监控并阻止风险行为	后将在该
☑ 记住本次操作,下次自动处理	
阻止执行	
允许执行	
限制风险行为(30)	





#### → 4: 软件安装拦截设置说明

您可在软件安装拦截设置中调整列表中软件的安装行为,还能在拦截设置中设置是否自

动阻止可识别软件的安装行为和自动阻止软件安装时是否显示通知弹窗。

0	安全设置		⇒	-	×
© ⊕	常规设置病毒防护	软件安装拦截 ————————————————————————————————————			
88	<mark>系统防护</mark> 系统加固 应用加固 风脸软件监控 软件安装兰截 隐私设备保护	拦截设置 自动处理规则 999+   自动阻止列表外已识别软件的安装行为   开启自动阻止软件安装时的弹窗通知			
•	浏览器保护 联网控制 自定义防护 <b>网络防护</b>				

功能	说明	
	自动阻止列表外已识别软件的	勾选后,除列表内软件外,将
拦截设置	安装行为	自动阻止所有已识别软件的安装行
		为。
	开启自动阻止软件安装时的弹	勾选后,自动阻止软件安装时
	窗通知	将在屏幕右下角弹出通知弹窗。
功能开关	开启:软件安装拦截功能生效。	
	关闭:软件安装拦截功能未生	
	效。	



★ 在火绒发现存在软件安装行为时会弹出提示弹窗, 当您勾选【记住本次操作, 下次自动

处理】时,会自动添加一条对应规则至列表中。

🤣 软件安装拦截	×
发现软件安装行为	
建议您立即阻止	
发起程序:  示例程序.exe	
软件名称:示例程序	
数字签名:示例程序网络科技有限公司	
推荐操作:如果不是您主动安装,建议您阻止	
🗌 记住本次操作,下次自动处理	
阻止(30)	
允许	

✓ 火绒弹出安装拦截提示弹窗时,不会区分软件的安装形式,无论是正常安装还是通过捆

绑、推广、静默或其他方式安装,都会统一提示用户。

✓ 软件安装拦截并非对软件安装包进行报毒,即使选"阻止"也不会删除软件安装包,您
 还可以再次执行,重新安装。

✓ 当您勾选了【开启自动阻止软件安装时的弹窗通知】勾选框时,并触发了自动阻止软件
 安装时,会弹出通知弹窗。





#### ⇒ 5: 隐私设备保护设置说明

#### ✓ 功能设置

您可在隐私设备保护设置中调整规则列表中程序的启动摄像头和麦克风的权限。



功能	说明				
摄像头保护	点击打开摄像头防护设置				
	仅通知	默认选择此项,选择后,新程序启			
		用摄像头时将进行提示。			
新程序启用摄像	自动阻止	选择此项后,将默认阻止新程序启			
头时处理方式		用摄像头。阻止后将创建一条自动处理			
		规则。			
	询问我	选择此项后,当有新程序启用摄像			
		头时,将弹窗询问您的操作。			



麦克风保护	点击打开麦克风防护设	
	置	
新程序启用麦克	仅通知	默认选择此项,选择后,新程序启
风时处理方式		用麦克风时将进行提示。
	自动阻止	选择此项后,将默认阻止新程序启
		用麦克风。阻止后将创建一条自动处理
		规则。
	询问我	选择此项后, 当有新程序启用麦克
		风时,将弹窗询问您的操作。
自动放行带有数	勾选后,带有数字签名的程序启用摄像头或麦克风时,将默认允	
字签名的程序	许,不会弹窗提示,但会创建一条自动处理规则。	
自动放行系统核	勾选后,带有系统程序启用摄像头或麦克风时,将默认允许,不	
心程序	会弹窗提示。	

 在设置为询问我时,火绒发现软件需要启动摄像头或麦克风时会弹出提示弹窗,当您勾

 选【记住本次操作,下次自动处理】时,会自动添加一条对应规则至列表中。





✓ 自定义规则




功能	说明
删除	删除所有选中规则
清除无效规则	删除所有无效的规则
	无效规则判定:对应路径下已无该程序。
添加	点击打开添加规则窗口,为指定程序配置访问摄像头和麦克风行
	为的自动处理规则。
导入	导入隐私设备保护的规则
导出	导出选中的隐私设备保护规则
编辑	编辑选中的规则

# ⇒ 7:浏览器保护设置说明

您可在浏览器保护设置中锁定浏览器首页、以及是否开启网购保护。

0	安全设置		⇒ – ⊡ ×	<
0 1	常规设置病毒防护	<b>浏览器保护</b> 保护浏览器首页和搜索不被篡改		
88	系统防护	保护浏览器首页     锁定浏览器首页为: 例如:www.huorong.cn		
	应用加固 风险软件监控 软件安装拦截 险私设备保护 浏览器保护 联网控制	网购保护 ✓ 当访问购物网站时提示		
	自定义防护 <b>网络防护</b>			



功能	说明
保护浏览器首页	保护浏览器的首页不被恶意篡改
网购保护	当访问购物网站时,进行提示和保护。
功能开关	开启:浏览器保护功能生效。
	关闭:浏览器保护功能未生效。



#### → 8: 联网控制设置说明

您可在联网控制设置中调整列表中程序的联网行为、添加新的程序联网规则、以及调整 当前联网控制触发时机。

0	安全设置		⇒	-	0	×
© 1	常规设置病毒防护	联网控制 管控应用程序的联网行为				
88	<ul> <li>新統防护</li> <li>系統加固</li> <li>应用加固</li> <li>风险软件监控</li> <li>約件法表出報</li> </ul>	功能设置     自动处理规则 999+       新程序联网时 ①       ● 自动允许       ● 自动乱止				
Ð	软件交装上或 隐私设备保护	<ul> <li>● 询问我</li> <li>高级设置</li> <li>□ 自动放行有数字签名的程序 ①</li> <li>☑ 自动放行系统核心程序 已放行的系统核心程序列表</li> </ul>				

✓ 功能设置



功能	说明					
	允许联网	除了您阻止联网的程序以外,均默认允许其				
		他程序联网。允许后将创建一条自动处理规则。				
	阻止联网	除了您允许联网的程序以外,均默认阻止其				
		他程序联网。阻止后将创建一条自动处理规则。				
新程序联网	询问我	未在自动处理规则中设置的其他程序联网				
时		时,会增加弹窗提示。此项默认勾选。				
	自动放行带有数字	选择阻止联网或询问我时启用,勾选后自动				
	签名的程序	允许所有带有数字签名的程序联网。				
	自动放行系统核心	选择阻止联网或询问我时启用,勾选后自动				
	程序	允许系统核心程序联网。此项默认勾选。				
功能开关	开启:联网控制功能生效。					
	关闭:联网控制功能未生效。					

★ 当【联网设置】中选择询问我(默认选项)时,每当有联网控制以外的程序发送联网请求,联网控制会增加弹窗提示(见下图),您可根据需要选择对这个动作的处理方式。您也可勾选【记住本次操作】后点击允许/阻止,添加一条允许/阻止联网的规则到联网控制中。您仍可在联网控制中修改或删除此规则。





✓ 自定义规则





功能	说明			
搜索	支持通过程序路径来搜索规则,并实时展示搜索结果。			
编辑	编辑选中的规则			
删除	删除所有选中的规则			
导入	点击后选择需要导入的规则,点击确定等待规则导入完成。			
导出	将导出所有选中的规则, 点击后选择保存位置点击确定, 等待导出			
	完成。			
清除无效规则	删除所有无效的规则			
	无效规则判定:对应路径下已无该程序。			
添加	点击打开添加程序窗口(见下图)			

点击【添加规则】,弹出添加程序窗口(见下图)。此窗口支持拖拽添加程序,还支持 使用通配符来批量添加需要控制联网的程序。

🤣 添加规则				×
输入程序路径,支持通配符(必填)			选择程序	
程序	ং প	历史流量		
实例程序 3tch64		25.10M		
xxxx程序 C:\Windows\apppatch\AppPatch64		25.10M		
s\System		1.42M		
		25.10M		
		1.42M		
处理方式: 🔘 自动允许 🥥 自动阻止 🔲 记录日志		保存	取消	



功能	说明
处理方式	为程序的联网行为选择处理方式,默认勾选阻止联网。
是否记录日志	复选框,勾选即针只针对本条数据的规则被触发时,记录相关日 志。
保存	保存当前规则,添加至规则列表中。
取消	退出添加规则状态,不保存当前规则。

#### → 9: 自定义防护设置说明

您可在自定义防护设置中添加自定义防护规则,以及查看并管理所有您创建的自定义规则。自定义防护设置中包含自定义规则和自动处理两部分内容。您可点击顶部的标签,切换页面。

#### ✓ 自定义防护-自定义规则

第一步:点击【自定义规则】(见下图),进入自定义规则页面。



0	安全设置										
0	常规设置	自定义	义防护								
Đ	病毒防护	对文件	、注册	表以及程序的	执行	进行控制以	及防护				
88	系统防护			自定义规则	999	+/999+			自动	处理规则 999	
	系统加固										添加
	应用加固			规则名称		发起程序		父进租	i t	保护对象	
	风险软件监控			自定义规则1			∍ îllu	(1)-	xxxx程序	共3条	
	软件安装拦截										
	摄像头保护			自定义规则2			e		xxxx桯序 C:\Windo	共1条	
	浏览器保护	~		白空义抑制3		<b></b> *		00		#7冬	
	联网控制							00			
	自定义防护										
$\oplus$	网络防护										

功能	说明					
搜索	支持通过规则名称和发起程序搜索规则,并实时展示搜索结果。					
状态开关	开关亮色表示规则启用,开关灰色表示规则未启用。					
编辑	编辑选中的规则					
删除	删除所有选中的规则					
导入	点击后选择需要导入的规则,点击确定等待规则导入完成。					
导出	将导出所有选中的规则,点击后选择保存位置点击确定,等待导出					
	完成。					
添加	点击添加规则进入自定义防护规则添加页面 (见下图)					
功能开关	开启: 自定义防护功能生效。					
	关闭:自定义防护功能未生效。					



# 第二步:添加自定义规则

💋 添加自定义	规则		D	×
*规则名称: 👔	自定义规则1			
发起程序 ①:			高级设置	
*发起精	序: C:\Windows\Bro	vserCore\en-US\Adobe Illustrator CC 2023	选择程序	
发起程序命令	符: *			
*发起程序父进	程: *		选择程序	
父进程命令	行: *			
*保护对象:	添加保护对象		对象路径 Q	
□ 保护类型	2  年	● 保护动作	操作	
文件规则	C:\	x文件 Program Files (	编辑 删除	
□ 执行规则		x程序 · · · · · · · · · · · · · · · · · · ·	编辑  删除	
□ 注册表规	۳IJ 📄 🕬 C:\	x注册表 🛛 创建 🗹 读取 🗌 修改 🗌 删除 Program Files (	编辑 删除	
处理方式: 🔘 🕯	甸河我 🔿 自动阻止 🛛		子 取消	
功能		说明		
<b>抑则复杂</b> 古毗计抑则复杂 司修改				
MGKU 1111				
发起程序		选择需要控制操作的程序,支持通配符。		
搜索		可针对保护对象内容进行搜索		
保护对象	添加保护对	添加阻止程序操作的对象,点击后显示汤	和保护对象	页
	象	面(见下图)。		
	保护动作	点击可勾选保护的动作		
编辑		编辑选中的保护对象		
	删除	删除选中的保护对象		
有程序触	询问我	弹出提示弹窗,让您来自主处理威胁。		
犯以上规	直接阻止	火绒将直接阻止程序操作,不再弹窗询问	您。	



则时	
保存	保存当前规则,添加至自定义防护规则列表中。
取消	点击关闭弹窗,不保存规则。

第三步:添加规则-添加保护对象

🤣 打开										
$\leftrightarrow \rightarrow \uparrow$ C:\Users\lion\music $\checkmark$										
🔜 计算机	名称	≑ 修改日期 ≎	类型 🗘	大小 🗘						
💼 下载		2021/02/25 14:22	PNG图像	294.1MB						
> = 我的桌面	o Program Fils	2021/12/25 23:59	本地磁盘	24КВ						
> 🚞 文件1	党 ପ୍ର	2021/02/25 14:22	PNG图像	294.1MB						
🚞 文件		2021/12/25 23:59	本地磁盘	24KB						
文件	logo	2021/02/25 14:22	PNG图像	294.1MB						
> 🚺 我的音乐		2021/12/25 23:59	本地磁盘	24KB						
🛄 我的桌面	rc 🔤	2021/02/25 14:22	PNG图像	294.1MB						
🔀 我的图片	🦲 列表1	2021/12/25 23:59	PNG图像	294.1MB						
	📄 logo	2021/12/25 23:59	本地磁盘	24KB						
文件名:		JSON 文件(*.json) >	打开	取消						

功能		说明
	文件规则	选择需要保护的文件,勾选需要阻止的操作,保护动作
		可选择创建、读取、写入、删除四项操作限制。
伊拉对各	注血主抑则	选择需要保护的注册表,勾选需要阻止的操作,保护动
オテン家	江而夜秋火	作可选择创建、读取、写入、删除四项操作限制。
	执行规则	阻止程序运行其他程序,保护动作默认勾选执行且不可
	נאטאר רואנ	取消勾选。
保护动作	点击可勾	选保护的动作
保存		保存此保护对象,添加至保护对象列表中。



取消	关闭添加保护对象页,不保存该保护对象。

# ✓ 自定义防护-自动处理

自动处理规则必须有对应的自定义规则才能生效,自动处理规则的优先级高于自定义规则。点击【自动处理】(见下图)进入自动处理规则页面。

0	安全设置										₽	— c	x נ
0	常规设置		自定义	防护									
Ð	病毒防护		对文件.	、注册:	表以及程序的	功抗行进行	う 控制じ	及防护					
88	系统防护			1	自定义规则	999+/99				自动处理规则	999+		
	系统加固					父进程、			۹.			添加	a
	应用加固				发起程序		父进和	₹¢	保护家	对象			处理
	风险软件监控					llu	2</th <th>xxxx程序 C:\Windo</th> <th>共3条</th> <th></th> <th></th> <th></th> <th></th>	xxxx程序 C:\Windo	共3条				
	摄像头保护					Pre	*/20	xxxx程序 C\Windo	共1条				
	浏览器保护						8		共2条				
	联网控制				<u> </u>		-						
¢	自定义防护												
₽	网络防护												
功能	<del>ل</del> الا	说明											
搜索	R	支持通过	してお	已程序	亨搜索规	见则,	并词	时展示	搜索	结果。			

删除	删除所有选中的规则
导入	点击后选择需要导入的规则,点击确定等待规则导入完成。
导出	将导出所有选中的规则,点击后选择保存位置点击确定,等待导出完成。



## 添加自动处理规则:

💋 添加自动处	理规则	- ×
发起程序 ①:		高级设置 ^
* 发起程	序: C:\Windows\Brov	vserCore\en-US\Adobe Illustrator CC 2023 选择程序
发起程序命令	行: *	
*发起程序父进	程: *	选择程序
父进程命令	行: *	
*保护对象:	泰加保护对象	删除所选 <b>保护对象路径 Q</b>
□ 保护类型	』 : 保护对象	保护动作 处理方式 操作     灰小切选一个保护的选择
□ 文件规则	C:\Progra	
□ 执行规则	□ xxxx程序	☑ 执行 命令行:C\WIND\Dll.exe
_	xxxx:=m	ŧ.
□ 执行规则	C:\Progra	~ ▽ 执行 命令行:C\WIND…\DII.exe
		保存 取消
功能		说明
发起程序		选择需要阻止操作的程序,支持通配符。
搜索		可针对保护对象内容进行搜索
保护对象	添加	添加阻止程序操作的对象,点击后显示添加保护对象页
		国(见下图)。
	编辑	编辑选中的保护对象
	删除	删除选中的保护对象
	保护动作	点击可勾选保护的动作
保存		保存当前规则,添加至自动处理规则列表中。
取消		点击关闭弹窗,不保存规则。

第一步:点击【添加】,弹窗见下图。



🕗 添加自动处	理规则			
< 返回			🕛 自动处理规则	必须有对应的自定义规则才能生效
文件规则	1 注册表规	则执行规则		
您想要进行保护	啲文件(必选),支持输入追			
📮 计算机	名称		: 大小	≎ 类型 ≎
📴 下载	÷ 🗎 🔳		294.1MB	PNG图像
∨ 📮 我的桌	面 🔽 Progr	ram Fils	24КВ	本地磁盘
> 🗅 文	件1 ;		294.1MB	PNG图像
<b>立</b> 文	件		24КВ	本地磁盘
立 文	件 🛁 logo		294.1MB	PNG图像
> 🎦 我的音	乐 一		24КВ	本地磁盘
📑 我的桌	m E		294.1MB	PNG图像
🔀 我的图	片 🛁 列表1		24КВ	本地磁盘
未勾选保护动	作			
*保护的动作:	🗌 创建 📄 读取	■ 修改 ■ 删除		
				TRAVIC
处埋万式: 💛 🛛				保仔 取消
功能		说明		
功能		说明	白洪雷西四	
功能		说明 选择需要保护的文件	,勾选需要阻」	上的操作,可选择创
功能	文件规则	说明 选择需要保护的文件 建 速取 写 》 删除四	, 勾选需要阻」	上的操作,可选择创
功能	文件规则	说明 选择需要保护的文件 建、读取、写入、删除四:	,勾选需要阻」 项操作限制。	上的操作,可选择创
功能	文件规则	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册	,勾选需要阻」 项操作限制。 表,勾选需要P	上的操作,可选择创 且止的操作,可选择
功能	文件规则 注册表规则	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册 创建、读取、写入、删除	, 勾选需要阻」 项操作限制。 表, 勾选需要P 四项操作限制。	上的操作,可选择创 且止的操作,可选择
功能	文件规则 注册表规则	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册 创建、读取、写入、删除	,勾选需要阻」 项操作限制。 表,勾选需要P 四项操作限制。	上的操作,可选择创 且止的操作,可选择
功能	文件规则 注册表规则 执行规则	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册 创建、读取、写入、删除 阻止程序运行其他程	,勾选需要阻」 项操作限制。 表,勾选需要P 四项操作限制。 序	上的操作,可选择创 且止的操作,可选择
功能	文件规则 注册表规则 执行规则 保护动作	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册 创建、读取、写入、删除 阻止程序运行其他程 点击可勾选保护的动	,勾选需要阻」 项操作限制。 表,勾选需要阻 四项操作限制。 序 作	上的操作,可选择创 且止的操作,可选择
功能 保护对象	文件规则 注册表规则 执行规则 保护动作	说明 选择需要保护的文件 建、读取、写入、删除四 选择需要保护的注册 创建、读取、写入、删除 阻止程序运行其他程 点击可勾选保护的动	,勾选需要阻」 项操作限制。 表,勾选需要P 四项操作限制。 序 作	上的操作,可选择创 阻止的操作,可选择
功能 保护对象 保存	文件规则         注册表规则         执行规则         保护动作	<ul> <li>说明</li> <li>选择需要保护的文件</li> <li>建、读取、写入、删除四:</li> <li>选择需要保护的注册:</li> <li>创建、读取、写入、删除</li> <li>创建、读取、写入、删除</li> <li>阻止程序运行其他程</li> <li>点击可勾选保护的动。</li> <li>保存此保护对象规则</li> </ul>	,勾选需要阻」 项操作限制。 表,勾选需要陷 四项操作限制。 序 作	上的操作,可选择创 且止的操作,可选择
功能 保护对象 保存	文件规则         注册表规则         执行规则         保护动作	<ul> <li>说明</li> <li>选择需要保护的文件</li> <li>建、读取、写入、删除四:</li> <li>选择需要保护的注册:</li> <li>创建、读取、写入、删除</li> <li>创建、读取、写入、删除</li> <li>【阻止程序运行其他程</li> <li>点击可勾选保护的动;</li> <li>保存此保护对象规则</li> </ul>	,勾选需要阻」 项操作限制。 表,勾选需要P 四项操作限制。 序 作	上的操作,可选择创 且止的操作,可选择

第二步:添加自动处理规则-添加保护对象。



★ 自动处理规则,除了可手动添加外,还可自动添加。当有程序触发自定义防护规则时, 会弹出提示弹窗,当您勾选【记住本次操作,下次自动处理】选择允许/阻止后,将会自动 添加一条对应规则至自动处理中。

🦪 自定义防护	×
发现程序试图操作 注册表防护项目	
发起程序: 嘱 <u>示例程序.exe</u> 防护项目:自定义规则	结束进程
操作目标:[读取]C:\Users\five\Desktop 序.exe	\示例程
记住本次操作,下次自动处理	
阻止(30)	
允许	



#### → 1: 网络入侵拦截设置说明

您可在设置中调整当发生黑客入侵或其他网络入侵行为时火绒需进行的操作。





#### 关闭:网络入侵拦截功能未生效。

#### → 2: 对外攻击拦截设置说明

您可在设置中调整当本机发生对外攻击行为时火绒需进行的操作。



0	安全设置	ج	F	0	×
0	常规设置	网络入侵拦截			
Ð	病毒防护	在网络层拦截漏洞攻击、黑客入侵等威胁			
88	系统防护				
	网络防护	X197-X11-#1 在网络层拦截本机对外部计算机的漏洞攻击等行为			
	基础防护	○ 仅记录 ◎ 自动阻止			
	横向渗透防护				
	寒愈攻击的护 恶意网址拦截	在网络层拦截潜在后门攻击			
		Web服务保护			
		针对高店Web服务属洞参选攻击进行防护			
功俞	<del>ک</del>	说明			
仅订	录	不阻止对外攻击行为,只在安全日志中记录攻击行为。			
自动	<b>办</b> 处理	阻止对外攻击的行为,并且在安全日志中记录攻击行为。			
功俞	詽关	开启:对外攻击拦截功能生效。			
		关闭:对外攻击拦截功能未生效。			



#### ⇒ 3: 僵尸网络防护设置说明

0	安全设置		₽	-	٥	×
© ±	常规设置 病毒防护	网络入侵拦截 🥌 在网络层拦截漏洞攻击、黑客入侵等威胁 〇 仅记录 🛛 ④ 自动阻止				
85 ()	条500000 网络防护 基础防护	对外攻击拦截 ————————————————————————————————————				
	橫向渗透防护 暴破攻击防护 恶意网址拦截	<ul> <li> <b>僵尸网络防护</b> <ul> <li></li></ul></li></ul>				
		Web服务保护 针对高危Web服务漏洞渗透攻击进行防护 〇 仅记录 ④ 自动阻止				

当您的计算机被非法远程控制时火绒需进行的操作。

功能	说明
仅记录	在安全日志中记录计算机被远程控制
自动处理	阻止远程控制,并记录至安全日志中。
功能开关	开启:僵尸网络防护功能生效。
	关闭:僵尸网络防护功能未生效。



#### ➡ 4: Web 服务保护设置说明

当黑客对安装了服务器软件的计算机发起攻击,入侵您计算机的服务器软件时火绒需进

行的操作。

💋 安全设置		≂ – ⊡ X
<ul><li>② 常规设置</li><li>① 病毒防护</li></ul>	网络入侵拦截 ─── 在网络层拦截漏洞攻击、黑客入侵等威胁 ○ 仅记录 ● 自动阻止	
88系统防护 ① 网络防护 基础防护	对外攻击拦截 ————————————————————————————————————	
横向渗透防护 暴破攻击防护 恶意网址拦截	<ul> <li>         ・個 戸 网络防护         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	
	Web服务保护 针对高危Web服务漏洞渗透攻击进行防护 〇 仅记录 ④ 自动阻止	

功能	。
仅记录	不阻止对服务器软件的攻击,只在安全日志中记录攻击行为。
自动处理	阻止对服务器软件的攻击,并在安全日志中记录攻击行为。
功能开关	开启:Web 服务保护功能生效。
	关闭:Web 服务保护功能未生效。

#### → 5:横向渗透防护设置说明

横向渗透防护开启后,触犯防护规则时默认设置为自动阻止。根据不同情况您也可调整 为触犯防护规则时仅记录。同时也可以添加信任规则,对指定 IP 发起的横向渗透行为进行



## 放过。

🥠 安全设置		≂ – □ ×
<ul> <li>⑦ 常规设置</li> <li>(土) 病毒防护</li> </ul>	<b>横向渗透防护</b>	
BI 系统防护	功能设置 信任列表 999+	
⊕ 网络防护	防护项目	触犯防护规则时: 🔿 仅记录 🙁 自动阻止
基础防护 横向渗透防护	<b>默认共享访问</b> 阻止对本机Windoors默认共享访问	
暴破攻击防护 恶意网址拦截	远程服务创建 阻止通过RPC远程创建本机服务	
	远程计划任务创建 阻止通过RPC远程创建本机计划任务	
	远程注册表篡改 阻止通过RPC远程修改本机注册表	
	远程打印机添加 阻止通过RPC远程添加打印机驱动	
	远程MMC调用 对远程调用本机MMC20.Application的行为进行拦截	
	远程DCOM调用 对远程调用本机DCOM组件的行为进行拦截	
	远程WMI调用 对远程调用本机WMI的行为进行拦截	

功能	<b>说明</b>
防护开关	某条防护项目的防护开关开启与关闭,影响着该防护项目的生效与 否。
仅记录	发现横向渗透行为时,只在安全日志中记录渗透行为。
自动处理	发现横向渗透行为时,在安全日志中记录并阻止渗透行为。
功能开关	开启:横向渗透防护功能生效。
	关闭:横向渗透防护功能未生效。



# ✓ 信任列表

0	安全设置					6	⇒ –	
0	常规设置	横向渗透防护 🛑						
Đ	病毒防护	在网络剧	昙拦截横向渗透攻击 					
88	系统防护		功能设置	信任列表	999+			
	网络防护							添加
	基础防护		远程IP地址		适用范围	备注	操作	
	横向渗透防护		192.168.1.111		开启3项防护	远程计划任务创建	编辑	
	暴破攻击防护		192.168.1.166		开启5项防护	MMC远程执行拦截	编辑	
	恶意网址拦截		192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	1.111	全部开启	MMC远程执行拦截	编辑	
			192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	.1.111	全部开启	MMC远程执行拦截	编辑	
			192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	.1.111	全部开启	远程计划任务创建	编辑	
			192.168.1.121;192.168	.1.111	全部开启	MMC远程执行拦截	编辑	

功能	说明
编辑	编辑选中的规则
删除	删除所有选中的规则
添加	点击添加规则打开规则添加页面 (见下图)
导入	导入信任规则
导出	导出选中的信任规则



(● 唯同的参战的 ¹¹ ************************************		
通貨P           第419年期,"红***9649/2005年月月11/1628           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1           1 <th></th> <th></th>		
修理時期: %2; *5% #P038### *68           * IBRDE           WIT           IBRDE           IBRDE		"远程IP
		多个IP使用","或";"分隔,IP范围使用"-"设置
通用范围         ● 新山共学访问         ● ジロビガ共構築         ● ジロビガ共和         ● ジロビガス 「「         ● ジロ 「「         ● ジロ 「         ● ジロ		
新以共要訪問             『受援発効理             『受援光物任务创建             『ご愛光物任务创建             『ご愛光物任务创建             『ご愛光物任务创建             『ご愛光物任务创建             『ご愛光物任务创建             『ご愛光物任务创建             『ご愛光物任务の対             『             『「「「「「「「「」」」」」		
Image: Control to define the set of the se		
新注         第注         「?!" ! #夏貸触地人送送         健用         支援用         设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用 "_" )         和 Ipv6 (可缩写),支持 CDIR,多个 IP 请用 ";"、"," 分隔; IP         范围使用 "-" 设置。         5日         支置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一页。         新注         方便您辨识规则,可不填写。         我有添加规则页面,返回至信任列表页,不保存规则。		
新建       「デビ:共学校第近人社社工         (保存)       取消         (成何)       (現一)         (支留需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用 "_")         (和 Ipv6 (可缩写), 支持 CDIR, 多个 IP 请用 ";"、","分隔; IP         (范围使用 "-" 设置。         (期范围)         (支留触犯横向渗透行为时信任的操作范围。适用范围至少勾选一页。         (項。         (項。         (項。         (項)         (項)         (項)         (項)         (項)         (項)         (現)         (項)         (現)         (項)         (現)         (現)<		
Image: Image		· · · · · · · · · · · · · · · · · · ·
展存         取消           b能         说明           b提 IP         设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"")           和 Ipv6 (可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP           范围使用"-"设置。           5期范围         设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一页。           5注         方便您辨识规则,可不填写。           存存         保存此规则           英词添加规则页面,返回至信任列表页,不保存规则。		示例:共享设备连入验证
成期         说明           韓星 IP         设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用 "_")           和 Ipv6 (可缩写),支持 CDIR,多个 IP 请用 ";"、","分隔; IP           范围使用 "-" 设置。           5用范围         设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一 项。           就         方便您辨识规则,可不填写。           保存         保存此规则           以調         关闭添加规则页面,返回至信任列表页,不保存规则。		
b能         说明                • 送置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"_")               · 公置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"_")                 和 Ipv6 (可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP             范围使用"-" 设置。               范围使用"-" 设置。                 印范围               · 公置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一             项。                 新               方便您辨识规则,可不填写。                 · "             · 经国本规则               · 公面和知识页面,返回至信任列表页,不保存规则。		保存 取消
分能     说明            • 设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"_")         和 lpv6 (可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP         范围使用"-"设置。             • 5.目前使用"-"设置。             • 5.目前意思             • 这置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一         项。             • 我             • 百度您辨识规则,可不填写。             • 保存此规则             • 英词添加规则页面,返回至信任列表页,不保存规则。		
我里 IP        设置需要访问的远程 IP 地址。可填写 IPv4 (表示范围使用"_")             和 Ipv6 (可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP             范围使用"-"设置。             印第范围             设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一             项。             新建             方便您辨识规则,可不填写。             保存此规则             我们添加规则页面,返回至信任列表页,不保存规则。	功能	说明
All Ipv6 (可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP         范围使用"-"设置。         資用范围         设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一项。         新注         方便您辨识规则,可不填写。         保存此规则         英词添加规则页面,返回至信任列表页,不保存规则。	远程 IP	设置需要访问的远程 IP 地址, 可填写 IPv4 (表示范围使用"")
和 lpv6 (可缩写),支持 CDIR,多个 IP 请用 ";"、 "," 分隔; IP         范围使用 "-" 设置。         資用范围       设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一项。         項。         許定         方便您辨识规则,可不填写。         保存此规则         英词添加规则页面,返回至信任列表页,不保存规则。	~~12 ···	
范围使用 "-" 设置。         第用范围       设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一项。         项。          新注       方便您辨识规则,可不填写。         保存       保存此规则         英词添加规则页面,返回至信任列表页,不保存规则。		和 lpv6(可缩写),支持 CDIR,多个 IP 请用";"、","分隔; IP
范围使用 "-" 设置。         5用范围       设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一项。         项。       功。         5注       方便您辨识规则,可不填写。         保存       保存此规则         メ闭添加规则页面,返回至信任列表页,不保存规则。		
新范围             设置触犯横向渗透行为时信任的操作范围。适用范围至少勾选一             项。                  新注               方便您辨识规则,可不填写。                 保存               保存此规则                 Xii               关闭添加规则页面,返回至信任列表页,不保存规则		范围使用"-"设置。
项。     项。       新加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加加	话田范围	设置触犯横向渗透行为时信任的操作范围,话田范围至少勾选—
项。       新注     方便您辨识规则,可不填写。       保存     保存此规则       X消     关闭添加规则页面,返回至信任列表页,不保存规则。	انترور با ب	
新注     方便您辨识规则,可不填写。       保存     保存此规则       大闭添加规则页面,返回至信任列表页,不保存规则。		项。
新江 方便您辨识规则,可不填写。 保存此规则 关闭添加规则页面,返回至信任列表页,不保存规则。	<b></b>	
<b>保存</b> 此规则 <b>X消</b> 关闭添加规则页面,返回至信任列表页,不保存规则。	备注	方便您辨识规则,可不填写。
<b>双消</b> 关闭添加规则页面,返回至信任列表页,不保存规则。	保存	保存此规则
双消 关闭添加规则页面,返回至信任列表页,不保存规则。		
	取消	关闭添加规则页面,返回至信任列表页,不保存规则。

#### → 6:暴破攻击防护设置说明

您可在暴破攻击设置中设置自动拦截哪些协议的暴破攻击,检测暴破攻击的灵敏度,临 时黑名单的生效时间和多源暴破攻击的处理方式。支持通过添加信任规则,对指定 IP 发起



## 的远程登录行为进行放过。

0	安全设置	₹	- 0 ×
© ⊕	常规设置病毒防护	<b>暴破攻击防护 ()</b> 发现暴破攻击行为,拦截潜在暴力破解攻击	
88	系统防护	功能设置 信任列表 999+ 临时黑名单 999+	
	网络防护		◎ 自动阻止
	基础防护 横向渗透防护	RDP 阻止通过RDP远程桌面协议对本机的暴破行为	
	暴破攻击防护 恶意网址拦截	SQL 阻止对本地SQL服务器的暴破行为	
		SMB 阻止通过SMB通讯协议对本机的暴破行为	
		RPC 阻止通过RPC远程调用协议对本机的暴破行为	
		发现多源暴破攻击时	
		1 指由多个攻击PP源对本地进行暴破攻击的场景,需要关闭本地端口才能拦截此关攻击	
		◎ 仅记录	

功能	说明
防护开关	防护开关开启与关闭,影响着该防护项目的生效与否。
触犯防护规则时	仅记录:不阻止暴破攻击行为,只在安全日志中记录攻击行为。
	自动阻止:阻止暴破攻击行为,并安全日志中记录攻击行为。
更多设置	打开设置窗口 (见下图)
功能开关	开启:暴破攻击防护功能生效。
	关闭:暴破攻击防护功能未生效。



✓ 更多设置

检测灵敏度

临时黑名单



日志中记录攻击行为,支持查看临时关闭的端口信息(见下图)。

灵敏度越高,可以检测到低频率的暴破攻击。

设置临时黑名单的生效时长, 默认 60 分钟。



# ✓ 临时关闭端口

0	临时关闭端口			×
C	一 本地端口	防护协议	生效时长	
	] 3389	SMB	59:24	
	] 211	SMB	59:24	
	] 3389	RPC	59:24	
	] 192	RPC	59:24	
删除				

功能	说明
删除	删除选中的规则

# ✓ 暴破攻击防护-信任列表

添加信任规则,对指定 IP 发起的远程登录行为进行放过。



0	安全设置							⇒ -	- o x
0	常规设置	暴破攻	な击防护 🌕						
Ð	病毒防护	发现暴	破攻击行为,拦截潜	在暴力破解	政击				
88	系统防护		功能设置	信任列表	999+	临时黑	名单 999+		
	网络防护								添加
	基础防护		信任IP		防护协议		备注	操作	
	横向渗透防护		fe80::98c0:b683:e48e	e:b40b	RDP,SMB		共享打印机多次连入失败	编辑	
	暴破攻击防护		192.168.1.166		SQL		物理机登录	编辑	
	恶意网址拦截		192.168.1.155-192.16	68.1.160	SMB		TCP 端口扫描攻击	编辑	

功能	<b>说明</b> 
编辑	编辑选中的规则
删除	删除选中的所有规则
导入	导入信任规则
导出	导出选中的所有信任规则
添加规则	添加信任规则(见下图)



🧦 添加规则	×
*信任IP	
多个IP使用","或";"分隔,IP范围使用"-"设置	Ġ
*防护协议	
RDP	
☑ SQL	
SWB	
✓ RPC	
备注	
· · · · · · · · · · · · · · · · · · ·	取消
	<u> </u>

功能	。
信任 IP	填写允许登录本机的远程 IP 地址
防护协议	选择允许采用的暴力破解攻击类型
备注	方便您辨识规则,可不填写。
保存	保存当前规则,添加至规则列表中。
取消	退出添加规则状态,不保存当前规则。



# ✓ 临时黑名单

0	安全设置					5. 5.	≂ – ⊡ ×
0	常规设置	暴破攻	女击防护 🦲				
Đ	病毒防护	发现暴	破攻击行为,拦截潜在	E暴力破解攻击			
88	系统防护		功能设置	信任列表 99	99+ 临时黑名单	999+	
	网络防护						
	基础防护		攻击IP		防护协议	生效时长	操作
	橫向渗透防护		198.168.1.1		SMB	59:24	
	暴破攻击防护		198.168.1.248		SMB	59:24	
	恶意网址拦截		198.168.1.1		RPC	59:24	
			198.168.1.248		RPC	59:24	
ፓታ		说明					
-75		00.13					
删降	除		删除选中的规	见贝」			



## → 7:恶意网址拦截设置说明

	安全设置		⇒		×
0	常规设置	恶意网址拦截 🦲			
Đ	病毒防护	自动阻止木马、欺诈、钓鱼类等网址			
88	系统防护	功能设置 自定义规则 999+			
۲	网络防护	网址分类			
	基础防护	段 木马、盗号			
	橫向渗透防护				
	暴破攻击防护				
	恶意网址拦截	1 钓鱼、仿置		0	
		ゆ 流氓软件		$\bigcirc$	
_					

调整需要拦截的网址类型,同时还能自定义添加需要拦截的网站。

# ✓ 功能设置

功能	说明
状态开关	开启:自动阻止打开该类网址。
	关闭:允许打开该类网址。
开关状态	开启:恶意网址拦截功能生效。
	关闭:恶意网址拦截功能未生效。



# ✓ 自定义规则

💋 安全设置					≂ – ⊡ ×
◎ 常规设置	恶意风	列址拦截 🦲			
土 病毒防护	自动阻	山上木马、欺诈、智	的鱼类等网址		
品 系统防护		功能设置	自定义规则 999+		
⊕ 网络防护					添加
基础防护		规则名称		\$ 状态	≎ 操作
橫向渗透防护		自定义网址		<u> </u>	编辑 删除
暴破攻击防护		自定义网址			编辑 删除
恶意网址拦截		自定义网址			编辑 删除
		自定义网址			编辑 删除
		自定义网址		$\bigcirc$	编辑  删除
		自定义网址			编辑 删除
		自定义网址			编辑  删除
		自定义网址		$\bigcirc$	编辑 删除
		自定义网址		$\bigcirc$	编辑  删除
		自定义网址			编辑 删除
		自定义网址			编辑 删除
功能	说明				
功能 编辑	说明编辑选口	中的规则			
功能 编辑 删除	说明 编辑选中 删除所有	中的规则 有选中的规	!见リ		
功能 编辑 删除 导入	说明       编辑选中       删除所有       点击后谈	中的规则 可选中的规 选择需要导	则 ² 入的规则,点击	确定等待规则导入	、完成。
功能 编辑 删除 导入 导出	说明       编辑选中       删除所有       点击后说       将导出所	中的规则 可选中的规 选择需要导 所有选中的	则 ² 入的规则,点击 1规则,点击后进	确定等待规则导入 5择保存位置点击码	、完成。 确定,等待导出
功能 编辑 删除 导入 导出	说明       编辑选中       删除所有       点击后说       将导出所       完成。	中的规则 可选中的规 选择需要导 所有选中的	则 ² 入的规则,点击 D规则,点击后进	确定等待规则导入 F择保存位置点击码	、完成。 确定,等待导出
功能 编辑 删除 导入 导出	说明       编辑选中       删除所有       点击后说       将导出所       完成。	中的规则 有选中的规 选择需要导 所有选中的	则 ² 入的规则,点击 1规则,点击后进	确定等待规则导入	<b>、完成。</b> 确定,等待导出
功能         編辑         删除         号入         导出         添加	<ul> <li>说明</li> <li>编辑选中</li> <li>删除所有</li> <li>点击后说</li> <li>将导出所</li> <li>完成。</li> </ul>	中的规则 有选中的规 选择需要导 所有选中的	则 ² 入的规则,点击 D规则,点击后进 动规则添加页面(	确定等待规则导入 5择保存位置点击码 见下图)	<b>、完成。</b> 确定,等待导出
功能         編辑         删除         日         导入         导出         添加         状态开关	说明         編辑选中         删除所有         点击后说         将导出所         完成。         开启:	中的规则 有选中的规 选择需要导 所有选中的 和规则打开 自动阻止打	则 之的规则,点击 动规则,点击后进 动规则添加页面( 开该类网址。	确定等待规则导入 5择保存位置点击码 见下图)	<b>、完成。</b> 确定,等待导出



#### ✓ 添加自定义规则

	🤊 恶意	网址拦截	×
	自定义网	1址1	
	多个网址	L通过换行进行区分,支持通配符 '*' '>' (必填 )	
		保存取消	]
功能	ŝ	说明	
保存	Z	保存当前规则,添加至规则列表中。	
取消	Í	关闭添加规则窗口,不保存当前规则。	

# ≻ 安全日志

安全日志是安全杀毒软件的一项基础功能,您可以利用安全日志查看一段时间内电脑的 安全情况,也可以根据日志来分析电脑遇到的问题。

# ● 功能介绍

您可在首页的主菜单中找到【安全日志】或首页的安全日志快捷入口(见下图),打开 安全日志。





在安全日志中,您可根据需要自定义时间、类别、功能过滤您要查看的内容。

1	🕗 安全日志				-	D	×
	时间: 2023/01/17 — 202	3/01/27 🖯   类别: 🖆	全部 / 全部		质	副新	
	时间	类别	功能	概要			
	2023/01/22 13:02:55	其他	升级日志	自动更新成功,版本号:5.0.33.13			
	2023/01/22 13:02:55	病毒防护	病毒查杀	快速扫描,发现0个风险项			
	2023/01/22 13:30:12	系统防护	联网控制	iexplore.exe触犯网络防护规则 , 已阻止			
	2023/01/22 13:02:55	网络防护	网络入侵拦截	受到【远程地址】的网络攻击,已阻止			
	2023/12/22 00:02:55	访问控制	网站内容控制	尝试访问【网址信息】,已阻止			
	2023/12/22 00:02:55	安全工具	漏洞修复	已手动安装n个漏洞补丁			
	病毒库时间:2021-01-1216:3 开始时间:2021-01-01000 总计用时:00:02:10 扫描对象:85116 扫描文件:84901 发现风险:0 已处理风险:0 查看更多	2					
	总项目数:5			清除	日志	导出日	志
功	能	说明					
肟	间	提供了【全	部】、【今天】、	【最近三天】、【最近七	天】	•	【最
		近三十天】、自	1定义时间段。				



类别	根据情况选择要查看的列表,共有全部、病毒防护、系统防护、
	网络防护、高级防护、访问控制、安全工具、其他等。
功能	根据选择的【类别】显示需要具体查看的功能
概要	阐述当前日志的简单情况
查看详情	选中需要查看的日志,即可在下方显示该条日志详情。
刷新	刷新当前日志列表
总项目数	根据筛选条件,显示符合当前条件的日志总条数。
清空本页日志	将符合筛选条件的日志全部清空
导出本页日志	将符合筛选条件的日志全部导出



您可在常规设置-日志和隔离设置中修改安全日志的保存天数、日志存储大小限制。



/ 🕖 安全设置		≂ – ⊡ ×
◎ 常规设置	安全日志设置	
基础设置	超过存储限制或磁盘已满时自动移除最早的日志	
查杀设置	日志保存天数不超过 7 天	
日志和隔离	□ 存储大小限制 1024 MB	
软件升级	后卤尺沙垩	
王 病毒防护		
88 系统防护		
⊕ 网络防护		

功能	说明
日志保存天数	根据需要选择日志保存天数,可自定义保存天数。
存储大小限制	根据需要设置是否限制日志存储大小,勾选后,超过存储限制
	或磁盘已满时自动移除最早的日志。

# > 软件升级

# ● 升级方式

当前您可通过以自动升级或手动升级的方式来升级火绒至最新版本。

#### → 1: 自动升级

火绒默认使用自动升级,当火绒需要升级更新时,会自动与火绒服务器连接,进行升级, 让软件时刻保持在最新状态,以保证病毒库和功能都是当前最完善的。当火绒升级完毕时会



弹出弹窗提示您。



部分升级完成后需重启电脑,火绒推荐您在保存好文件后及时重启电脑,保证火绒各项 功能与配置均处于最新状态,以最大程度保护好您的电脑。

💋 火绒安全	×
升级完成,部分功能需要重启电脑后生效	
最新版本:6.0.0.1	
最新病毒库:2023-05-23 16:12	
	重启

→ 2: 手动升级

您也可通过手动升级,检查是否有可升级的内容。在下拉菜单中点击【检查升级】、首 页的检查更新快捷入口(见下图)、以及右键火绒托盘程序,在右键快捷菜单中点击【检查 升级】弹出在线升级弹窗,进行检查升级。



0		<b>)</b>
•	已保护 <mark>21</mark> 天	
Ŧ	火绒正在保护您的电脑	
කී	快速查杀	
	<ul> <li></li></ul>	12-
IJ		
0	①         E         I         I           检查更新         安全日志         信任区         隔离区         版本: 6.0.0.0         病毒库:	: 2023-03-18 09:56
	〇 火 3 K 支 王 已保护您的计算机 2324 天 进入	
	✓ X3x支主 已保护您的计算机 2324 天 进入 适 适 信任区 隔离区	
	●保护您的计算机 2324 天       进入         ●保护您的计算机 2324 天       进入         ●       ●         信任区       隔离区         ●       ●         安全日志       ●	
	Y 3x 52 至         已保护您的计算机 2324 天       进入         Image: Constraint of the state of the stat	
	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	

当有可升级的内容时,在线升级会显示:检查到最新版本(见下图),您可点击【立即 升级】按钮来完成软件升级。





升级完成若是需要重启电脑,将弹出重启提示(见下图)。





为防止您设置手动更新后,出于各种原因,在一周内未进行病毒库更新,导致病毒库内数据与最新数据不一致。系统将会在一周后您重启火绒或重启电脑时进行托盘消息提示。



● 软件升级设置说明

在安全设置中,常规设置-软件升级可进入软件升级的设置页面。可对软件升级方式、 升级提示、升级代理进行调整修改。


🤣 安全设置		≂ – ⊡ ×
<ul> <li>常规设置</li> <li>基础设置</li> </ul>	升级方式 ◎ 自动升级 〇 手动升级	
查杀设置 日志和隔离 软件升级	升级提示	
土 病毒防护	代理设置	
品 系统防护	□ 指定服务器代理 网络测试	
⊕ 网络防护		

功能	说明
升级方式	您可根据需要选择升级方式,火绒推荐您保持自动升级。
升级提示	勾选后自动更新完成时将不再弹出升级完成的提示弹窗
代理设置	勾选指定服务器代理后,填写地址、端口、账号、密码。将使用代
	理服务器来连接火绒升级服务器。
网络测试	测试当前使用的连接方式能否连接上火绒服务器



总结

在《用户操作手册》中我们详细地为您介绍了火绒安全软件各项功能的使用方法,不管 您是家庭用户还是专业技术人员,火绒都能为您提供合适的病毒防护模式,全方位保护您的 计算机安全。如果您在火绒的使用中遇到任何问题或有任何意见与建议,您都可以通过前往 火绒官方论坛进行反馈: <u>https://bbs.huorong.cn/</u>

最后,再次感谢您选择火绒安全软件!